Disponibilidad de vSphere

Actualización 2
Modificado el 13 de agosto de 2020
VMware vSphere 6.5
VMware ESXi 6.5
vCenter Server 6.5



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de Disponibilidad de vSphere

Disponibilidad de vSphere describe soluciones que ofrecen continuidad del negocio, incluido cómo establecer vSphere® High Availability (HA) y vSphere Fault Tolerance.

Audiencia prevista

La información es para cualquiera que desee proporcionar continuidad del negocio a través de las soluciones vSphere HA y Fault Tolerance. La información de este manual es para administradores expertos de los sistemas Windows y Linux que están familiarizados con la tecnología de máquinas virtuales y las operaciones de centro de datos.

Las instrucciones para las tareas en esta guía se basan en vSphere Web Client. También puede realizar la mayoría de las tareas en esta guía con la nueva instancia de vSphere Client. La terminología, la topología y el flujo de trabajo de la interfaz de usuario de la nueva instancia de vSphere Client están estrechamente alineados con los mismos aspectos y elementos de la interfaz de usuario de vSphere Web Client. Puede aplicar las instrucciones de vSphere Web Client a la nueva instancia de vSphere Client, a menos que se indique lo contrario.

Nota No todas las funcionalidades de vSphere Web Client se implementaron para vSphere Client en vSphere 6.5. Para obtener una lista actualizada de las funcionalidades no compatibles, consulte la Guía sobre actualizaciones de las funcionalidades de vSphere Client en http://www.vmware.com/info?id=1413.

Información actualizada

Esta *Disponibilidad de vSphere* se actualiza con cada versión del producto o cuando es necesario.

Esta tabla muestra el historial de actualizaciones de la *Disponibilidad de vSphere*.

Revisión	Descripción
10 de agosto de 2020	En VMware, valoramos la inclusión. Para fomentar este principio entre nuestros clientes, nuestros partners y nuestra comunidad interna, estamos reemplazando parte de la terminología en nuestro contenido. Hemos actualizado esta guía para eliminar el lenguaje no inclusivo.
1 de junio de 2018	■ Se agregó información actualizada para configurar MSCS para alta disponibilidad. Consulte Configurar MSCS para alta disponibilidad.
3 de mayo de 2018	Versión inicial.

Continuidad del negocio y minimización del tiempo de inactividad

1

El tiempo de inactividad, ya sea planificado o no planificado, acarrea costes considerables. Sin embargo, tradicionalmente las soluciones para asegurar mayores niveles de disponibilidad fueron costosas, difíciles de implementar y complicadas de administrar.

Con el software de VMware resulta más simple y menos costoso proporcionar mayores niveles de disponibilidad para aplicaciones importantes. Con vSphere, es posible aumentar el nivel básico de disponibilidad proporcionado para todas las aplicaciones, así como ofrecer niveles más altos de disponibilidad de forma más fácil y rentable. Con vSphere, puede:

- Proporcionar mayor disponibilidad, independientemente del hardware, del sistema operativo y de las aplicaciones.
- Reducir el tiempo de inactividad planificado para operaciones comunes de mantenimiento.
- Proporcionar la recuperación automática en caso de errores.

vSphere permite reducir el tiempo de inactividad planificado, evitar el tiempo de inactividad planificado y recuperarse rápidamente de interrupciones.

Este capítulo incluye los siguientes temas:

Reducir el tiempo de inactividad planificado

El tiempo de inactividad planificado suele representar más del 80 % del tiempo de inactividad del centro de datos. El mantenimiento de hardware, la migración de servidores y las actualizaciones de firmware requieren tiempo de inactividad de los servidores físicos. Para minimizar el impacto de este tiempo de inactividad, las organizaciones se ven obligadas a retrasar el mantenimiento hasta encontrarse con períodos de tiempo de inactividad inconvenientes y difíciles de programar.

vSphere permite que las organizaciones puedan reducir en gran medida el tiempo de inactividad planificado. Debido a que las cargas de trabajo en un entorno de vSphere se pueden mover de forma dinámica a servidores físicos diferentes sin tiempo de inactividad o interrupción de servicio, el mantenimiento de servidores se puede realizar sin que se requiera tiempo de inactividad para aplicaciones y servicios. Con vSphere, las organizaciones pueden:

- Eliminar el tiempo de inactividad de las operaciones de mantenimiento comunes.
- Eliminar ventanas de mantenimiento planificadas.
- Realizar mantenimiento en cualquier momento sin interrumpir a los usuarios y servicios.

La funcionalidad vSphere vMotion® y Storage vMotion en vSphere permiten que las organizaciones reduzcan el tiempo de inactividad planificado debido a que las cargas de trabajo en un entorno de VMware se pueden mover de forma dinámica a diferentes servidores o a un almacenamiento subyacente diferente sin interrupción del servicio. Los administradores pueden realizar operaciones de mantenimiento más rápidas y completamente transparentes, sin que se vean obligados a programar períodos de mantenimiento inconvenientes.

Evitar el tiempo de inactividad no planificado

Aunque los hosts ESXi proporcionan una robusta plataforma para ejecutar aplicaciones, las organización también deben protegerse contra el tiempo de inactividad no planificado debido a errores de hardware o aplicaciones. vSphere crea importantes capacidades en la infraestructura de centro de datos que puede ayudarle a prevenir tiempo de inactividad no planificado.

Estas capacidades de vSphere forman parte de infraestructura virtual y son transparentes para el sistema operativo y aplicaciones que se ejecutan en máquinas virtuales. Estas características las pueden configurar y utilizar todas las máquinas virtuales de un sistema físico, lo que reduce el costo y la complejidad que implica proporcionar mayor disponibilidad. Las capacidades clave están integradas en vSphere:

- Almacenamiento compartido. Elimina puntos únicos de error mediante el almacenamiento de archivos de máquina virtual en almacenamiento compartido, como SAN de canal de fibra o iSCSI, o NAS. El uso del reflejo de SAN y las características de replicación se pueden utilizar para mantener copias actualizadas de un disco virtual en sitios de recuperación ante desastres.
- Formación de equipos de interfaz de red. Ofrece tolerancia de errores de tarjetas de red individuales.
- Múltiples rutas alternativas. Tolera errores de ruta de almacenamiento.

Además de estas funcionalidades, las características de vSphere HA y Fault Tolerance pueden minimizar o eliminar el tiempo de inactividad no planificado proporcionando una recuperación rápida ante las interrupciones y una disponibilidad continua, respectivamente.

vSphere HA ofrece una rápida recuperación desde interrupciones

vSphere HA aprovecha varios hosts ESXi configurados como clúster para proporcionar una rápida recuperación desde interrupciones y alta disponibilidad rentable para aplicaciones que se ejecutan en máquinas virtuales.

vSphere HA protege la disponibilidad de aplicaciones de las siguientes formas:

- Protege contra error de un servidor mediante el reinicio de las máquinas virtuales en otros hosts dentro del clúster.
- Protege contra errores de aplicaciones mediante una supervisión continua de una máquina virtual y su restablecimiento en caso de que se detecte un error.
- Protege contra errores de accesibilidad al almacén de datos mediante el restablecimiento de máquinas virtuales afectadas en otros hosts que aún tienen acceso a sus almacenes de datos.
- Protege a las máquinas virtuales contra el aislamiento de la red mediante el restablecimiento de dichas máquinas en caso de que su host se aísle en la red de administración o de vSAN. Esta protección se proporciona incluso si la red se ha particionado.

A diferencia de otras soluciones de clúster, vSphere HA proporciona la infraestructura para proteger todas las cargas de trabajo con la infraestructura:

- No necesita instalar software especial dentro de la aplicación o máquina virtual. Todas las cargas de trabajo cuentan con protección de vSphere HA. Después de configurar vSphere HA, no se requieren acciones para proteger nuevas máquinas virtuales. Están se encuentran protegidas automáticamente.
- Puede combinar vSphere HA con vSphere Distributed Resource Scheduler (DRS) para proteger contra errores y para proporcionar equilibrio de carga entre los hosts dentro de un clúster.

vSphere HA posee varias ventajas por sobre las soluciones de conmutación por error tradicionales:

Instalación mínima

Después de instalar un clúster de vSphere HA, todas las máquinas virtuales del clúster obtienen compatibilidad para conmutación por error sin una configuración adicional.

Menor costo e instalación de hardware

La máquina virtual actúa como un contenedor portátil para las aplicaciones y puede moverse entre hosts. Los administradores evitan configuraciones duplicadas para varias máquinas. Cuando usa vSphere HA, debe tener suficientes recursos para realizar conmutación por error en la cantidad de hosts que desea proteger con vSphere HA. Sin embargo, el sistema VMware vCenter Server® administra automáticamente recursos y configura clústeres.

Mayor disponibilidad de aplicaciones

Cualquier aplicación que se ejecuta dentro de una máquina virtual tiene acceso a mayor disponibilidad. Debido a que la máquina virtual puede recuperarse de errores de hardware, todas las aplicaciones que se inician en el arranque tienen mayor disponibilidad sin que haya mayores necesidades informáticas, incluso si la aplicación no es en sí una aplicación en clúster. Mediante la supervisión y la respuesta a latidos de VMware Tools y el restablecimiento de máquinas virtuales sin capacidad de respuesta, protege contra fallas del sistema operativo invitado.

Integración de DRS y vMotion

Si hay error en un host y las máquinas virtuales se restablecen en otros hosts, DRS puede proporcionar recomendaciones de migración o migrar máquinas virtuales para asignación de recursos equilibrados. Si se produce error en uno o ambos hosts de origen y destino de una migración, vSphere HA puede ayudar a recuperarse de dicho error.

vSphere Fault Tolerance proporciona disponibilidad continua

vSphere HA ofrece un nivel de protección básico para sus máquinas virtuales mediante un reinicio de ellas en caso de un error del host. vSphere Fault Tolerance proporciona un mayor nivel de disponibilidad, permitiendo que los usuarios puedan proteger cualquier máquina virtual contra un error del host sin perder datos, transacciones o conexiones.

Fault Tolerance proporciona disponibilidad continua al asegurar que los estados de las máquinas virtuales principales y secundarias sean idénticos en cualquier punto de la ejecución de instrucciones de la máquina virtual.

Si se produce un error en el host que ejecuta la máquina virtual principal o en el que ejecuta la máquina virtual secundaria, se produce una conmutación por error inmediata y transparente. El host ESXi en funcionamiento se convierte de forma sencilla en el host de la máquina virtual principal sin perder conexiones de red ni transacciones en curso. Con una conmutación por error transparente, no hay pérdida de datos y las conexiones de red se mantienen. Después de producirse una conmutación por error transparente, reaparece una nueva máquina virtual secundaria y se vuelve a establecer redundancia. El proceso completo es transparente, está completamente automatizado y se produce aunque vCenter Server no esté disponible.

Proteger vCenter Server Appliance con vCenter High Availability

vCenter High Availability (vCenter HA) es una herramienta que no solo protege contra errores de host y hardware, sino también contra errores de aplicaciones de vCenter Server. Al usar la conmutación por error automatizada de activa a pasiva, vCenter HA admite alta disponibilidad con un mínimo tiempo de inactividad.

Opciones de implementación de vCenter HA

vCenter HA protege vCenter Server Appliance. No obstante, Platform Services Controller proporciona autenticación, administración de certificados y licencias para vCenter Server Appliance. Como resultado, es necesario garantizar la alta disponibilidad de Platform Services Controller. Tiene estas opciones.

- Implemente un nodo activo con una instancia integrada de Platform Services Controller. Como parte del proceso de clonación, Platform Services Controller y todos sus servicios también se clonan. Como parte de la sincronización del nodo activo al nodo pasivo, se actualiza Platform Services Controller en el nodo pasivo.

  Cuando se produce la conmutación por error del nodo activo al nodo pasivo, Platform Services Controller está disponible en el nodo pasivo y también está disponible todo el entorno.

- Implemente al menos dos instancias de Platform Services Controller y colóquelas detrás de un equilibrador de carga.

  Cuando se produce la conmutación por error del nodo activo al nodo pasivo, el nodo pasivo sigue apuntando al equilibrador de carga. Cuando una de las instancias de Platform Services Controller deja de estar disponible, el equilibrador de carga dirige las solicitudes a la segunda instancia de Platform Services Controller.

Consulte Opciones de implementación de vCenter HA.

Opciones de configuración de vCenter HA

vCenter HA se configura desde vSphere Web Client. El asistente de configuración proporciona estas opciones.

Opción	Descripción
Básico	La opción básica clona el nodo activo al nodo pasivo y nodo testigo, y configura los nodos por el usuario. Si el entorno cumple con uno de los siguientes requisitos, puede usar esta opción. ■ La instancia de vCenter Server Appliance que se convierte en el nodo activo administra su propio host ESXi y su propia máquina virtual. Esta configuración a veces se denomina instancia de vCenter Server autoadministrada. ■ La instancia de vCenter Server Appliance administrada por otra instancia de vCenter Server (vCenter Server de administración) y ambas instancias de vCenter Server se deben encontrar en el mismo dominio de vCenter Single Sign-On. Eso significa que ambos utilizan una instancia de Platform Services Controller externa y ambos ejecutan vSphere 6.5. Consulte Configurar vCenter HA con la opción básica.
Avanzado	La opción avanzada ofrece más flexibilidad. Esta opción se puede utilizar si el entorno cumple con los requisitos de hardware y software. Si selecciona esta opción, tiene la responsabilidad de clonar el nodo activo al nodo pasivo y nodo testigo. También debe realizar algunos ajustes en la configuración de redes. Consulte Configurar vCenter HA con la opción avanzada.

Proteger vCenter Server con VMware Service Lifecycle Manager

La disponibilidad de vCenter Server depende de VMware Service Lifecycle Manager.

Si se produce un error en un servicio de vCenter, VMware Service Lifecycle Manager lo reinicia. VMware Service Lifecycle Manager supervisa el estado de los servicios y, al detectar un error, toma medidas de corrección preconfiguradas. El servicio no se reinicia si se producen errores en varios intentos de corrección.

Crear y usar clústeres de vSphere HA

2

Los clústeres de vSphere HA permiten que una colección de hosts ESXi funcionen en conjunto, de manera que, como grupo, proporcionen mayores niveles de disponibilidad para máquinas virtuales de lo que puede proporcionar de forma individual cada host ESXi. Cuando planifique la creación y el uso de un nuevo clúster de vSphere HA, las opciones que seleccione afectarán la manera en que el clúster responde a los errores de los hosts o las máquinas virtuales.

Antes de crear un clúster de vSphere HA, debe saber cómo identifica vSphere HA los errores y el aislamiento de hosts y cómo responder a estas situaciones. También debe saber de qué forma funciona el control de admisión para que pueda elegir la directiva que se ajusta a sus necesidades de conmutación por error. Después de establecer un clúster, puede personalizar su comportamiento con opciones avanzadas y optimizar su rendimiento siguiendo estas prácticas recomendadas.

Nota Es posible que reciba un mensaje de error cuando intente usar vSphere HA. Para obtener información sobre los mensajes de error relacionados con vSphere HA, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1033634.

Este capítulo incluye los siguientes temas:

Funcionamiento de vSphere HA

vSphere HA ofrece alta disponibilidad para máquinas virtuales agrupando en un clúster las máquinas virtuales y los hosts en los que residen. Se supervisan los hosts en el clúster y, en caso de un error, las máquinas virtuales en un host con errores se reinician en hosts alternativos.

Cuando se crea un clúster de vSphere HA, automáticamente se elige un único host como el host principal. El host principal se comunica con vCenter Server y supervisa el estado de todas las máquinas virtuales protegidas y de los hosts secundarios. Es posible que haya diferentes tipos de errores del host, y el host principal debe detectar y corregir apropiadamente el error. El host principal debe distinguir entre un host con errores y uno que está en una partición de red o que ha quedado aislado de la red. Para determinar el tipo de error, el host principal utiliza la verificación de latidos de la red y del almacén de datos.



Clústeres de vSphere HA
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ynopbsu2/uiConfId/49694343/)

Hosts principales y secundarios

Cuando agrega un host a un clúster de vSphere HA, se carga un agente al host que se configura para que se comunique con otros agentes del clúster. Cada host del clúster funciona como host principal o host secundario.

Cuando vSphere HA está habilitado para un clúster, todos los hosts activos (aquellos que no están en modo de espera o mantenimiento ni están desconectados) participan en una elección para seleccionar el host principal del clúster. El host que monta la mayor cantidad de almacenes de datos tiene una ventaja en la elección. Normalmente, solo existe un host principal por clúster y todos los otros hosts son secundarios. Si el host principal genera errores, se apaga o se coloca en modo de espera o se quita del clúster, se realiza una nueva elección.

El host principal de un clúster tiene varias responsabilidades:

- Supervisar el estado de los hosts secundarios. Si un host secundario genera errores o no se puede acceder a él, el host principal identifica qué máquinas virtuales deben reiniciarse.
- Supervisar el estado de energía de todas las máquinas virtuales protegidas. Si una máquina virtual genera errores, el host principal se asegura de que se reinicie. Mediante el uso de un motor de selección de ubicación local, el host principal también determina dónde debe realizarse el reinicio.
- Administrar las listas de hosts del clúster y máquinas virtuales protegidas.
- Actuar como la interfaz de administración de vCenter Server con el clúster e informar el estado del clúster.

Los hosts secundarios contribuyen principalmente con el clúster ejecutando máquinas virtuales a nivel local, supervisando sus estados de tiempo de ejecución y notificando actualizaciones de estado al host principal. Un host principal también puede ejecutar y supervisar máquinas virtuales. Tantos los hosts secundarios como los principales implementan las funciones de supervisión de máquinas virtuales y de aplicaciones.

Una de las funciones que realiza el host principal es orquestar reinicios de máquinas virtuales protegidas. Una máquina virtual se protege mediante un host principal después de que vCenter Server observe que el estado de energía de la máquina virtual ha cambiado de apagado a encendido en respuesta a una acción del usuario. El host principal mantiene activa la lista de máquinas virtuales protegidas en los almacenes de datos del clúster. Un host principal elegido recientemente utiliza esta información para determinar qué máquinas virtuales hay que proteger.

Nota Si desconecta un host de un clúster, las máquinas virtuales registradas en ese host quedan sin protección de vSphere HA.

Tipos de error de host

El host principal de un clúster de VMware vSphere® High Availability es el responsable de detectar el error de los hosts secundarios. Según el tipo de error detectado, es posible que las máquinas virtuales que se ejecutan en los hosts necesiten someterse a conmutación por error.

En un clúster de vSphere HA, se detectan tres tipos de errores de hosts:

- Error. Un host deja de funcionar.
- Aislamiento. Un host se aísla de la red.
- Partición. Un host pierde conectividad de red con el host principal.

El host principal supervisa la ejecución de los hosts secundarios en el clúster. Esta comunicación ocurre a través del intercambio de latidos de la red cada segundo. Cuando el host principal deja de recibir estos latidos de un host secundario, comprueba la ejecución del host antes de declarar que este tiene errores. La comprobación de ejecución que realiza el host principal se hace para determinar si el host secundario está intercambiando latidos con uno de los almacenes de datos. Consulte Latidos del almacén de datos . Igualmente, el host principal comprueba si el host responde a los pings de ICMP enviados a sus direcciones IP de administración.

Si un host principal no puede comunicarse directamente con el agente en un host secundario, este no responde a los pings de ICMP. Si el agente no envía latidos, se considera que tiene un error. Las máquinas virtuales del host se reinician en hosts alternativos. Si ese host secundario está intercambiando latidos con un almacén de datos, el host principal supone que el host secundario está en una partición de red o está aislado de la red. Por lo tanto, el host principal sigue supervisando el host y sus máquinas virtuales. Consulte Particiones de red .

El aislamiento de la red del host se produce cuando un host sigue en ejecución, pero ya no puede observarse tráfico de los agentes de vSphere HA en la red de administración. Si un host deja de observar este tráfico, intenta hacer ping a las direcciones de aislamiento del clúster. Si también se produce un error al hacer ping, el host declara que está aislado de la red.

El host principal supervisa las máquinas virtuales que están ejecutándose en un host aislado. Si el host principal observa que las máquinas virtuales se desconectan y este es responsable por las máquinas virtuales, las reinicia.

Nota Si se asegura de que la infraestructura de la red es lo suficientemente redundante y que hay al menos una ruta de acceso de red disponible todo el tiempo, es menos probable que se produzca un aislamiento de la red del host.

Errores de Proactive HA

Se produce un error de Proactive HA ante un error en un componente del host, lo que ocasiona una pérdida de redundancia o un error no grave. Sin embargo, esto no afecta el comportamiento funcional de las máquinas virtuales que residen en el host. Por ejemplo, si se produce un error en el suministro de energía del host, pero hay otros suministros de energía disponibles, se trata de un error de Proactive HA.

Si se produce un error de Proactive HA, puede automatizar la medida de corrección realizada en la sección Disponibilidad de vSphere de vSphere Web Client. Las máquinas virtuales del host afectado pueden ser evacuadas a otros hosts y el host se coloca en modo de cuarentena o en modo de mantenimiento.

Nota El clúster debe usar vSphere DRS para que la supervisión de errores de Proactive HA funcione.

Determinar respuestas a problemas del host

Si se produce un error en un host y es necesario reiniciar sus máquinas virtuales, puede controlar el orden en el cual se reinician mediante la configuración de prioridad de reinicio de máquinas virtuales. También puede configurar de qué forma responde vSphere HA si los hosts pierden conectividad de red de administración con otros hosts mediante el uso de la configuración de respuesta para el aislamiento del host. También se consideran otros factores cuando vSphere HA reinicia una máquina virtual después de un error.

La siguiente configuración se aplica a todas las máquinas virtuales en el clúster en caso de un error o aislamiento del host. También es posible configurar excepciones para máquinas virtuales específicas. Consulte Personalizar una máquina virtual individual .

Respuesta de aislamiento del host

La respuesta para el aislamiento del host determina lo que ocurre cuando un host en un clúster de vSphere HA pierde sus conexiones de red de administración, pero sigue ejecutándose. Puede usar la respuesta para aislamiento para que vSphere HA apague las máquinas virtuales que se ejecutan en un host aislado y las reinicie en un host que no esté aislado. Las respuestas para aislamiento del host requiere que Estado de supervisión de hosts esté habilitado. Si está deshabilitado, también se suspenden las respuestas para aislamiento del host. Un host determina

que está aislado cuando no puede comunicarse con los agentes que se ejecutan en los otros, y no puede hacer ping a sus direcciones de aislamiento. Después, el host ejecuta su respuesta de aislamiento. Las respuestas son Apagar y reiniciar máquinas virtuales o Desactivar y reiniciar máquinas virtuales. Puede personalizar esta propiedad para máquinas virtuales individuales.

Nota Si la configuración de prioridad de reinicio de una máquina virtual se establece en Deshabilitada, no se realiza ninguna respuesta para aislamiento del host.

Para usar la configuración Desactivar y reiniciar máquina virtual, debe instalar VMware Tools en el sistema operativo invitado de la máquina virtual. La desconexión de la máquina virtual ofrece la ventaja de que mantiene su estado. Desconectar es mejor que apagar la máquina virtual, lo que no purga los cambios más recientes al disco ni confirma transacciones. Las máquinas virtuales que se encuentran en proceso de desconexión ya no pueden realizar conmutación por error mientras se lleva a cabo la desactivación. Las máquinas virtuales que no se han desactivado en 300 segundos o en el tiempo que se haya especificado en la opción avanzada `das.isolationshutdowntimeout`, se apagan.

Después de que crea un clúster de vSphere HA, puede anular la configuración predeterminada del clúster para Prioridad de reinicio y Respuesta para aislamiento para máquinas virtuales específicas. Dichas anulaciones son útiles para máquinas virtuales que se utilizan para tareas especiales. Por ejemplo, puede que las máquinas virtuales que proporcionan servicios de infraestructura como DNS o DHCP tengan que apagarse antes que otras máquinas virtuales en el clúster.

Cuando un host se aísla o se particiona desde un host principal, y ese host principal no puede comunicarse con él mediante almacenes de datos de latidos, se puede producir una condición de "cerebro dividido" de la máquina virtual. En esta situación, el host principal no puede determinar que el host está activo y, por ello, lo declara inactivo. Luego, el host principal intenta reiniciar las máquinas virtuales que están ejecutándose en el host aislado o particionado. Este intento se realiza correctamente si las máquinas virtuales siguen ejecutándose en el host aislado o particionado, y si ese host perdió acceso a los almacenes de datos de las máquinas virtuales cuando se aisló o particionó. Entonces, existe una condición de cerebro dividido, ya que hay dos instancias de la máquina virtual. Sin embargo, solo una instancia puede leer o escribir en los discos virtuales de la máquina virtual. Se puede usar máquina virtual Protección de componentes de la máquina virtual para evitar esta condición de cerebro dividido. Cuando activa la VMCP con la configuración agresiva, supervisa la accesibilidad del almacén de datos de máquinas virtuales encendidas y desconecta aquellas que pierden acceso a sus almacenes de datos.

Para recuperarse de esta situación, ESXi genera una pregunta en la máquina virtual que ha perdido los bloqueos de discos para cuando el host salga del aislamiento y no pueda volver a adquirir dichos bloqueos. vSphere HA responde automáticamente a esta pregunta, lo que permite que la instancia de máquina virtual que perdió los bloqueos de discos se apague, con lo que queda solo la instancia que tiene los bloqueos de discos.

Dependencias de máquinas virtuales

Se pueden crear dependencias entre grupos de máquinas virtuales. Para ello, primero se deben crear grupos de máquinas virtuales en vSphere Web Client. En la pestaña **Configurar** del clúster, seleccione **Grupos de host/máquina virtual**. Una vez que se hayan creado los grupos, puede crear reglas de dependencia de reinicio entre los grupos. Para ello, desplácese hasta **Reglas de host/máquina virtual** y, en el menú desplegable, seleccione **Máquinas virtuales a máquinas virtuales**. Estas reglas pueden especificar que ciertos grupos de máquinas virtuales no se pueden reiniciar hasta que otros grupos de máquinas virtuales especificados estén listos antes.

Factores que se consideran para reiniciar máquinas virtuales

Después de un error, el host principal del clúster intenta reiniciar las máquinas virtuales afectadas mediante la identificación de un host que pueda encenderlas. Cuando se elige dicho host, el host principal considera varios factores.

Accesibilidad de archivos

Antes de poder iniciar una máquina virtual, sus archivos deben estar accesibles desde uno de los hosts del clúster activo con el que el principal puede comunicarse a través de la red.

Compatibilidad de máquinas virtuales y hosts

Si hay hosts accesibles, la máquina virtual debe ser compatible con al menos uno de ellos. La compatibilidad establecida para una máquina virtual incluye el efecto de cualquier regla de afinidad Máquina virtual-Host requerida. Por ejemplo, si una regla solo permite que se ejecute una máquina virtual en dos hosts, se contempla su colocación en aquellos dos hosts.

Reservas de recursos

De los hosts en los que puede ejecutarse la máquina virtual, al menos uno debe tener suficiente capacidad sin reservar para cumplir con la sobrecarga de memoria de la máquina virtual y cualquier reserva de recursos. Se consideran cuatro tipos de reservas: CPU, Memoria, vNIC y flash virtual. Igualmente, debe haber disponibles suficientes puertos de red para encender la máquina virtual.

Límites de hosts

Además de las reservas de recursos, una máquina virtual solo puede colocarse en un host si al hacerlo no se supera la cantidad máxima de máquinas virtuales permitidas o la cantidad de vCPU en uso.

Restricciones de características

Si se ha configurado la opción avanzada que requiere que vSphere HA aplique las reglas de antiafinidad entre máquinas virtuales, vSphere HA no infringe esta regla. También, vSphere HA no infringe ningún límite configurado por host para máquinas virtuales con Fault Tolerance.

Si ningún host satisface las consideraciones anteriores, el host principal emite un evento que indica que no hay suficientes recursos para que vSphere HA inicie la máquina virtual y vuelve a intentarlo cuando las condiciones del clúster han cambiado. Por ejemplo, si no se puede acceder a la máquina virtual, el host principal vuelve a intentarlo después de un cambio en la accesibilidad del archivo.

Supervisar máquina virtual y aplicaciones

Supervisión de máquina virtual reinicia máquinas virtuales individuales si los latidos de su VMware Tools no se reciben dentro de un tiempo establecido. De forma similar, Supervisión de aplicaciones puede reiniciar una máquina virtual si no se reciben los latidos para una aplicación que está en ejecución. Puede habilitar estas características y configurar la sensibilidad con la cual vSphere HA supervisa la incapacidad de respuesta.

Cuando habilita Supervisión de máquina virtual, este servicio (que usa VMware Tools) evalúa si se está ejecutando cada máquina virtual del clúster mediante la comprobación de latidos y actividad de E/S regulares del proceso de VMware Tools que se ejecuta dentro del invitado. Si no se reciben latidos ni actividad de E/S, lo más probable es que esto se deba a que hay errores en el sistema operativo invitado o que no se está asignando nada de tiempo a VMware Tools para completar las tareas. En dicho caso, el servicio Supervisión de máquina virtual determina que la máquina virtual generó errores y que esta se reinicia para restaurar el servicio.

En ocasiones, las máquinas virtuales o las aplicaciones que siguen funcionando adecuadamente dejan de enviar latidos. Para evitar restablecimientos innecesarios, el servicio Supervisión de máquina virtual también supervisa la actividad de E/S de una máquina virtual. Si no se reciben latidos dentro del intervalo de errores, se comprueba el intervalo de estadísticas de E/S (un atributo de nivel de clúster). El intervalo de estadísticas de E/S determina si se ha producido una actividad de disco o de red de la máquina virtual durante los dos minutos anteriores (120 segundos). Si no, la máquina virtual se restablece. Este valor predeterminado (120 segundos) se puede cambiar mediante la opción avanzada `das.iostatsinterval`.

Para habilitar Supervisión de aplicaciones, primero debe obtener el SDK adecuado (o usar una aplicación que sea compatible con Supervisión de aplicaciones de VMware) y usarlo para instalar latidos personalizados para las aplicaciones que desea supervisar. Después de que haya hecho esto, Supervisión de aplicaciones funciona de la misma forma que lo hace Supervisión de máquina virtual. Si los latidos de una aplicación no se reciben durante un tiempo especificado, su máquina virtual se reinicia.

Puede configurar el nivel de sensibilidad de supervisión. Una supervisión con alta sensibilidad da como resultado una conclusión más rápida de que se produjo un error. Aunque es improbable, la supervisión de alta sensibilidad podría llevar a la identificación incorrecta de errores cuando en realidad la máquina virtual o la aplicación siguen funcionando, pero no se han recibido latidos debido a factores como restricciones de recursos. La supervisión de baja sensibilidad da como resultado interrupciones más prolongadas en el servicio entre errores reales y el restablecimiento de máquinas virtuales. Seleccione una opción que sea un compromiso eficaz para sus necesidades.

Para especificar también valores personalizados tanto para la sensibilidad de supervisión como para el intervalo de estadísticas de E/S, puede activar la casilla **Personalizar**.

Tabla 2-1. Configurar Supervisión de máquina virtual

Configuración	Intervalo de errores (segundos)	Período de restablecimiento
Alto	30	1 hora
Mediano	60	24 horas
Bajo	120	7 días

Una vez que se detectan errores, vSphere HA restablece máquinas virtuales. El restablecimiento asegura que los servicios permanezcan disponibles. Para evitar restablecer máquinas virtuales de forma repetida para errores no transitorios, de forma predeterminada, las máquinas virtuales se restablecerán solo tres veces durante cierto intervalo de tiempo configurable. Después de que las máquinas virtuales se hayan restablecido tres veces, vSphere HA no realiza nuevos intentos para restablecer las máquinas virtuales después de errores posteriores hasta que haya transcurrido el tiempo especificado. Puede configurar la cantidad de restablecimientos mediante el uso de la configuración personalizada **Restablecimientos máximos por máquina virtual**.

Nota Las estadísticas de restablecimiento se borran cuando una máquina virtual se apaga y se vuelve a encender, o cuando se migra a otro host mediante el uso de vMotion. Esto hace que se reinicie el sistema operativo invitado, pero no es igual que un "restablecimiento" en el cual el estado de energía de la máquina virtual cambia.

protección de componentes de la máquina virtual

Si la opción Protección de componentes de la máquina virtual (VMCP) está habilitada, vSphere HA puede detectar errores de accesibilidad al almacén de datos y ofrecer recuperación automática para máquinas virtuales afectadas.

VMCP ofrece protección contra errores de accesibilidad al almacén de datos que pueden afectar a una máquina virtual que se ejecuta en un host en un clúster de vSphere HA. Cuando se produce un error de accesibilidad al almacén de datos, el host afectado ya no puede tener acceso a la ruta de acceso del almacén de datos para un almacén de datos específico. Puede determinar la respuesta que tomará vSphere HA para dicho error, que va desde la creación de alarmas de eventos hasta reinicios de máquinas virtuales en otros hosts.

Nota Cuando se utiliza la función Protección de componentes de la máquina virtual, los hosts ESXi deben ser versión 6.0 o posterior.

Tipos de error

Existen dos tipos de errores de accesibilidad al almacén de datos:

PDL

PDL (Pérdida permanente de dispositivos) es una pérdida irrecuperable de accesibilidad que se produce cuando un dispositivo de almacenamiento informa que el host ya no puede acceder almacén de datos. Esta condición no puede revertirse sin apagar las máquinas virtuales.

APD

APD (Todas las rutas de acceso inactivas) representa una pérdida de accesibilidad transitoria o desconocida o cualquier otro retraso sin identificar en el procesamiento de E/S. Este tipo de problema de accesibilidad es recuperable.

Configurar VMCP

La opción Protección de componentes de la máquina virtual se configura en vSphere Web Client. Vaya a la pestaña **Configurar**, haga clic en **Disponibilidad de vSphere** y seleccione **Editar**. En **Errores y respuestas**, puede seleccionar **Almacén de datos con PDL** o **Almacén de datos con APD**. Los niveles de protección de almacenamiento que escoja y las acciones de corrección de máquinas virtuales disponibles pueden ser diferentes dependiendo del tipo de error de accesibilidad de la base de datos.

Errores de PDL

En **Almacén de datos con PDL**, puede seleccionar **Emitir eventos** o **Apagar y reiniciar las máquinas virtuales**.

Errores de APD

Para respuesta a los eventos de APD es más completa y, en consecuencia, la configuración es más refinada. Puede seleccionar **Emitir eventos**, **Apagar y reiniciar las máquinas virtuales (directiva de reinicio conservadora)** o **Apagar y reiniciar las máquinas virtuales (directiva de reinicio agresiva)**

Nota Si las configuraciones Supervisión de hosts o Prioridad de restablecimiento de máquina virtual están deshabilitadas, VMCP no puede realizar restablecimientos de máquinas virtuales. Sin embargo, aún puede supervisarse el estado del almacenamiento y se pueden emitir eventos.

Particiones de red

Cuando se produce un error de red de administración para un clúster de vSphere HA, es posible que un subconjunto de los hosts del clúster no pueda comunicarse por la red de administración con los otros hosts. Pueden darse varias particiones en un clúster.

Un clúster particionado conduce a una protección de máquina virtual y funcionalidad de administración de clústeres degradados. Corrija el clúster particionado en cuanto sea posible.

- Protección de máquina virtual. vCenter Server permite que una máquina virtual se encienda, pero solo puede protegerse si se ejecuta en la misma partición que el host principal del cual es responsable. El host principal debe comunicarse con vCenter Server. Un host principal es responsable de una máquina virtual si ha bloqueado exclusivamente un archivo definido por el sistema en el almacén de datos que contiene el archivo de configuración de la máquina virtual.

- Administración de clústeres. vCenter Server puede comunicarse con el host principal, pero solo un subconjunto de los hosts secundarios. Como resultado, es posible que los cambios en la configuración que afecten a vSphere HA no tengan efecto hasta que se resuelva la partición. Este error podría dar como resultado que una de las particiones opere con la configuración antigua, mientras que otra usa la nueva.

Latidos del almacén de datos

Cuando el host principal en un clúster de VMware vSphere® High Availability no puede comunicarse con un host secundario a través de la red de administración, el host principal utiliza la verificación de latido del almacén de datos para determinar si el host secundario generó errores, está en una partición de red o está aislado de la red. Si el host secundario dejó de verificar latidos del almacén de datos, se considera que se generó un error y las máquinas virtuales se reinician en otra parte.

VMware vCenter Server® selecciona un conjunto de almacenes de datos preferidos para la verificación de latido. Esta selección se hace para maximizar la cantidad de hosts que tienen acceso a un almacén de datos de verificación de latido y minimizar la probabilidad de que el mismo servidor de LUN o NFS haga copia de seguridad de los almacenes de datos.

Puede usar la opción avanzada `das.heartbeatdsperhost` para cambiar la cantidad de almacenes de datos de latidos que haya seleccionado vCenter Server para cada host. El valor predeterminado es dos y el valor válido máximo es cinco.

vSphere HA crea un directorio en la raíz de cada almacén de datos que se utiliza tanto para verificación de latido del almacén de datos como para mantener activo el conjunto de máquinas virtuales protegidas. El nombre del directorio es `.vSphere-HA`. No elimine ni modifique archivos almacenados en este directorio, ya que esto puede tener un impacto en las operaciones. Debido a que más de un clúster podría usar un almacén de datos, se crean subdirectorios para este directorio para cada clúster. La raíz posee estos directorios y archivos y solo la raíz puede leer y escribir en ellos. El espacio de disco que utiliza vSphere HA depende de varios factores, entre los que se incluyen la versión de VMFS que hay en uso y la cantidad de hosts que utilizan el almacén de datos para verificación de latido. Con vmfs3, el uso máximo es de aproximadamente 2 GB y el uso típico es de cerca de 3 MB. Con vmfs5, el uso máximo y típico es de 3 MB. El uso de vSphere HA de los almacenes de datos agrega una sobrecarga insignificante y no afecta al rendimiento en otras operaciones del almacén de datos.

vSphere HA limita la cantidad de máquinas virtuales que pueden tener archivos de configuración en un solo almacén de datos. Consulte *Valores máximos de configuración* para conocer los límites actualizados. Si coloca más de esta cantidad de máquinas virtuales en un almacén de datos y las enciende, vSphere HA protege solo hasta el límite establecido de máquinas virtuales.

Nota No se puede usar un almacén de datos de vSAN para verificar latido del almacén de datos. Por lo tanto, si no hay otro almacenamiento compartido accesible para todos los hosts en el clúster, no podrá haber almacenes de datos de latidos en uso. Sin embargo, si tiene un almacenamiento al que puede acceder mediante una ruta de acceso de red alternativa que es independiente de la red de vSAN, puede usarlo para instalar un almacén de datos de latidos.

Seguridad de vSphere HA

vSphere HA se mejora a través de varias características de seguridad.

Selección de puertos de firewall abiertos

vSphere HA utiliza el puerto TCP y UDP 8182 para comunicación entre agentes. Los puertos de firewall se abren y cierran automáticamente para asegurar que estén abiertos solo cuando sea necesario.

Archivos de configuración protegidos mediante permisos del sistema de archivos

vSphere HA almacena información de configuración en el almacenamiento local o en ramdisk en caso de que no haya un almacén de datos local. Estos archivos se protegen mediante permisos del sistema de archivos y solo el usuario raíz puede acceder a ellos. Los hosts sin almacenamiento local solo son compatibles si los administra Auto Deploy.

Registro detallado

La ubicación donde vSphere HA coloca los archivos de registro depende de las versiones del host.

- Para hosts ESXi 5.x, vSphere HA escribe en syslog solo de manera predeterminada, por lo que los registros se colocan donde syslog está configurado para ponerlos. Los nombres de archivos de registro para vSphere HA vienen antecedidos con `fdm`, fault domain manager, que es un servicio de vSphere HA.
- Para hosts heredados de ESXi 4.x, vSphere HA escribe en `/var/log/vmware/fdm` en el disco local, así como en el syslog si está configurado.
- Para hosts ESX 4.x heredados, vSphere HA escribe en `/var/log/vmware/fdm`.

Inicios de sesión de vSphere HA seguros

vSphere HA inicia sesión en los agentes de vSphere HA mediante una cuenta de usuario, **vpxuser**, creada por vCenter Server. Esta cuenta es la misma que usa vCenter Server para administrar el host. vCenter Server crea una contraseña aleatoria para esta cuenta y cambia dicha contraseña de forma periódica. El período se establece con la configuración vCenter Server `VirtualCenter.VimPasswordExpirationInDays`. Los usuarios con privilegios administrativos en la carpeta raíz del host pueden iniciar sesión en el agente.

Comunicación segura

Toda la comunicación entre el agente de vCenter Server y de vSphere HA se realiza a través de SSL. La comunicación entre agentes también utiliza SSL, excepto para mensajes de elección, que se producen a través de UDP. Los mensajes de elección se verifican a través de SSL de manera que se evite elegir como host principal solo al host que ejecuta el agente

malicioso. En este caso, se emite un problema de configuración para el clúster de manera que el usuario tenga en cuenta el problema.

Verificación obligatoria del certificado SSL del host

vSphere HA requiere que cada host tenga un certificado SSL verificado. Cada host genera un certificado con autofirma cuando arranca por primera vez. Después, este certificado se puede volver a generar o reemplazar con uno emitido por una entidad. Si se reemplaza el certificado, es necesario volver a configurar vSphere HA en el host. Si un host se desconecta de vCenter Server después de que se actualiza su certificado y se reinicia el agente de host ESXi o ESX, entonces vSphere HA se vuelve a configurar automáticamente cuando el host se conecta de nuevo a vCenter Server. Si la desconexión no se produce debido a que en ese momento está deshabilitada la verificación del certificado SSL del host de vCenter Server, verifique el certificado nuevo y vuelva a configurar vSphere HA en el host.

Control de admisión de vSphere HA

vSphere HA utiliza el control de admisión para garantizar que se reserven recursos suficientes para la recuperación de máquinas virtuales cuando se produce un error en el host.

El control de admisión impone restricciones sobre el uso de recursos. No se permite ninguna acción con el potencial de infringir estas restricciones. Las acciones que es posible que no se permitan incluyen los siguientes ejemplos:

- Encendido de una máquina virtual
- Migración de una máquina virtual
- Aumento de la reserva de CPU o memoria de una máquina virtual

La base para el control de admisión de vSphere HA es la cantidad de errores de host que el clúster puede tolerar sin perder la capacidad de conmutación por error. La capacidad de conmutación por error del host puede establecerse de tres formas:

- Porcentaje de recursos del clúster
- Directiva de ranuras
- Hosts de conmutación por error dedicados

Nota Se puede deshabilitar el control de admisión de vSphere HA. Pero sin eso, no existe garantía de que se pueda reiniciar la cantidad esperada de máquinas virtuales después de un error. No deshabilite permanentemente el control de admisión.

Más allá de la opción de control de admisión elegida, también existe un umbral de reducción de recursos de máquina virtual. Esta configuración permite especificar el porcentaje de degradación de recursos que se tolerará, pero no está disponible a menos que se habilite vSphere DRS.

Se verifica el cálculo de la reducción de recursos tanto para CPU como para memoria. Se tiene en cuenta la memoria reservada de una máquina virtual y la sobrecarga de memoria para decidir si se permitirá encender, migrar o realizar cambios de reserva. La memoria real consumida por la máquina virtual no se considera en el cálculo, ya que la reserva de memoria no siempre se correlaciona con el uso de memoria real de la máquina virtual. Si el uso real supera la memoria reservada, la capacidad de conmutación por error es insuficiente y, como resultado, se produce una degradación en el rendimiento con la conmutación por error.

Establecer un umbral de reducción de rendimiento permite especificar la naturaleza de un error de configuración. Por ejemplo:

- El valor predeterminado es 100 %, lo que no produce advertencias.
- Si se reduce el umbral a 0 %, se genera una advertencia cuando el uso de un clúster excede la capacidad disponible.
- Si se reduce el umbral a 20 %, la reducción de rendimiento que puede tolerarse se calcula como `performance reduction = current utilization * 20%`. Cuando el uso actual menos la reducción de rendimiento excede la capacidad disponible, se emite un aviso de configuración.

Control de admisión de porcentaje de recursos del clúster

Puede configurar vSphere HA para realizar control de admisión mediante la reserva de un porcentaje específico de recursos de CPU y memoria del clúster para recuperación de errores del host.

Con este tipo de control de admisión, vSphere HA asegura que se reserve un porcentaje específico de recursos de CPU y memoria para conmutación por error.

Con la opción de porcentaje de recursos del clúster, vSphere HA aplica control de admisión de la siguiente forma:

1. Calcula los requisitos de recursos totales para todas las máquinas virtuales encendidas en el clúster.
2. Calcula los recursos totales del host disponibles para máquinas virtuales.
3. Calcula la capacidad actual de conmutación por error de la CPU y la capacidad actual de conmutación por error de la memoria para el clúster.
4. Determina si la capacidad actual de conmutación por error de la CPU o la capacidad actual de conmutación por error de la memoria es menor que la capacidad de conmutación por error configurada correspondiente (provista por el usuario).

   Si lo es, el control de admisión no permite la operación.

vSphere HA usa las reservas reales de las máquinas virtuales. Si una máquina virtual no tiene reservas, ello significa que la reserva es 0, y se aplica un valor predeterminado de memoria de 0 MB y una CPU de 32 MHz.

Nota La opción de porcentaje de recursos del clúster para el control de admisión también comprueba que haya al menos dos hosts habilitados para vSphere HA en el clúster (excluyendo los hosts que van a pasar a modo de mantenimiento). Si hay solo un host habilitado para vSphere HA, no se permite una operación, incluso si hay suficiente porcentaje de recursos disponibles. El motivo para esta comprobación adicional es que vSphere HA no puede realizar conmutación por error si hay un solo host en el clúster.

Calcular la capacidad actual de conmutación por error

Los requisitos de recursos totales para las máquinas virtuales encendidas constan de dos componentes: CPU y memoria. vSphere HA calcula estos valores.

- El componente de CPU, sumando las reservas de CPU de las máquinas virtuales encendidas. Si no ha especificado una reserva de CPU para una máquina virtual, se asigna un valor predeterminado de 32 MHz (este valor puede cambiarse usando la opción avanzada `das.vmcpuminmhz`.)
- El componente de memoria, sumando la reserva de memoria (más sobrecarga de memoria) de cada máquina virtual encendida.

Los recursos totales de host disponibles para máquinas virtuales se calculan agregando los recursos de CPU y memoria de los hosts. Estas cantidades son aquellas que están contenidas en el grupo de recursos raíz del host, no los recursos físicos totales del host. Los recursos que se van a usar para fines de virtualización no están incluidos. Solo se consideran los hosts que están conectados, que no están en modo de mantenimiento y que no tienen errores de vSphere HA.

La capacidad actual de conmutación por error de la CPU se calcula restando los requisitos de recursos totales de CPU de los recursos totales de CPU del host y dividiendo el resultado por los recursos totales de CPU del host. La capacidad actual de conmutación por error de la memoria se calcula de forma similar.

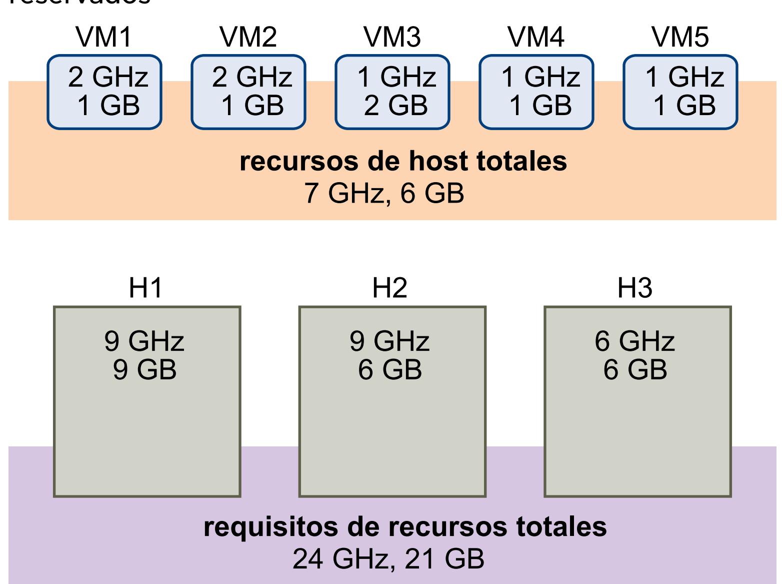
Ejemplo: Control de admisión mediante el uso de porcentaje de recursos del clúster

La forma en que se calcula y se usa la capacidad actual de conmutación por error con esta directiva de control de admisión se muestra con un ejemplo. Haga las siguientes suposiciones sobre un clúster:

- El clúster está compuesto de tres hosts, cada uno con una cantidad diferente de recursos de CPU y de memoria disponibles. El primer host (H1) posee 9 GHz de recursos de CPU disponibles y 9 GB de memoria disponible, en tanto que el host 2 (H2) tiene 9 GHz y 6 GB y el host 3 (H3) cuenta con 6 GHz y 6 GB.

- Existen cinco máquinas virtuales encendidas en el clúster con diferentes requisitos de CPU y memoria. La máquina virtual 1 necesita 2 GHz de recursos de CPU y 1 GB de memoria, en tanto que la máquina virtual 2 requiere 2 GHz y 1 GB, la máquina virtual 3, 1 GHz y 2 GB, la máquina virtual 4 necesita 1 GHz y 1 GB y la máquina virtual 5, 1 GHz y 1 GB.
- La capacidad configurada de conmutación por error para CPU y memoria está configurada para ambas en 25 %.

Figura 2-1. Ejemplo de control de admisión con la directiva Porcentaje de recursos del clúster reservados



Los requisitos de recursos totales para las máquinas virtuales encendidas son 7 GHz y 6 GB. Los recursos totales del host disponibles para máquinas virtuales son 24 GHz y 21 GB. Basado en esto, la capacidad actual de conmutación por error de la CPU es 70 % ((24 GHz - 7 GHz)/24 GHz). De forma similar, la capacidad actual de conmutación por error de la memoria es de 71 % ((21 GB - 6 GB)/21 GB).

Debido a que la capacidad configurada de conmutación por error del clúster está configurada en 25 %, un 45 % de los recursos totales de CPU del clúster y un 46 % de los recursos de memoria del clúster siguen disponibles para encender máquinas virtuales.

Control de admisión de directiva de ranuras

Con la opción de directiva de ranuras, el control de admisión de vSphere HA asegura que se puedan producir errores en una cantidad específica de hosts y que los recursos en el clúster sean suficientes para realizar conmutación por error en todas las máquinas virtuales desde esos hosts.

Al utilizar la directiva de ranuras, vSphere HA realiza el control de admisión de la siguiente forma:

1 Calcula el tamaño de ranura.

Una ranura es una representación lógica de los recursos de memoria y CPU. De forma predeterminada, tiene un tamaño para que satisfaga los requisitos para cualquier máquina virtual encendida en el clúster.

2 Determina cuántas ranuras puede mantener cada host en el clúster.

3 Determina la capacidad actual de conmutación por error del clúster.

   Esta es la cantidad de hosts que pueden tener errores y aún así dejar suficientes ranuras para que atienda a todas las máquinas virtuales encendidas.

4 Determina si la capacidad actual de conmutación por error es inferior a la capacidad configurada de conmutación por error (provista por el usuario).

   Si lo es, el control de admisión no permite la operación.

Nota Puede configurar un tamaño de ranura específico tanto para la CPU como la memoria en la sección de control de admisión de la configuración de vSphere HA en vSphere Web Client.

Calcular el tamaño de ranura



Tamaño de ranura y control de admisión de vSphere HA (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_q744qxvn/uiConfId/49694343/)

El tamaño de ranura consta de dos componentes: la CPU y la memoria.

- vSphere HA calcula el componente de CPU obteniendo la reserva de CPU de cada máquina virtual encendida y seleccionando el mayor valor. Si no ha especificado una reserva de CPU para una máquina virtual, se asigna un valor predeterminado de 32 MHz. Puede cambiar este valor usando la opción avanzada `das.vmcpuminmhz`.
- vSphere HA calcula el componente de memoria obteniendo la reserva de memoria, además de la sobrecarga de memoria, de cada máquina virtual encendida y seleccionando el mayor valor. No hay un valor predeterminado para la reserva de memoria.

Si su clúster contiene máquinas virtuales que tienen reservas mucho mayores que las otras, distorsionarán el cálculo del tamaño de ranura. Para evitar esto, puede especificar un límite superior para el componente de CPU o memoria del tamaño de ranura mediante el uso de las opciones avanzadas `das.slotcpuinmhz` o `das.slotmeminmb`, respectivamente. Consulte Opciones avanzadas de vSphere HA.

También puede determinar el riesgo de fragmentación de recursos en su clúster viendo la cantidad de máquinas virtuales que requieren varias ranuras. Esto se puede calcular en la sección de control de admisión de la configuración de vSphere HA en vSphere Web Client. Las máquinas virtuales pueden necesitar varias ranuras en caso de que haya especificado un tamaño de ranura fijo o un tamaño de ranura máximo usando opciones avanzadas.

Usar ranuras para calcular la capacidad actual de conmutación por error

Después de calcular el tamaño de ranura, vSphere HA determina los recursos de CPU y memoria de cada host que están disponibles para máquinas virtuales. Estas cantidades son aquellas que están contenidas en el grupo de recursos raíz del host, no los recursos físicos totales del host. Los datos de recursos para un host que utiliza vSphere HA se pueden encontrar en la pestaña **Resumen** del host en vSphere Web Client. Si todos los hosts de su clúster son iguales, estos datos se pueden obtener dividiendo las cifras de nivel de clúster por la cantidad de hosts. Los recursos que se van a usar para fines de virtualización no están incluidos. Solo se consideran los hosts que están conectados, que no están en modo de mantenimiento y que no tienen errores de vSphere HA.

Luego, se determina la cantidad máxima de ranuras que puede admitir cada host. Para hacerlo, la cantidad de recursos de CPU del host se divide por el componente de CPU del tamaño de ranura y el resultado se redondea hacia abajo. El mismo cálculo se hace para la cantidad de recursos de memoria del host. Estos números se comparan y el número menor es la cantidad de ranuras que puede admitir el host.

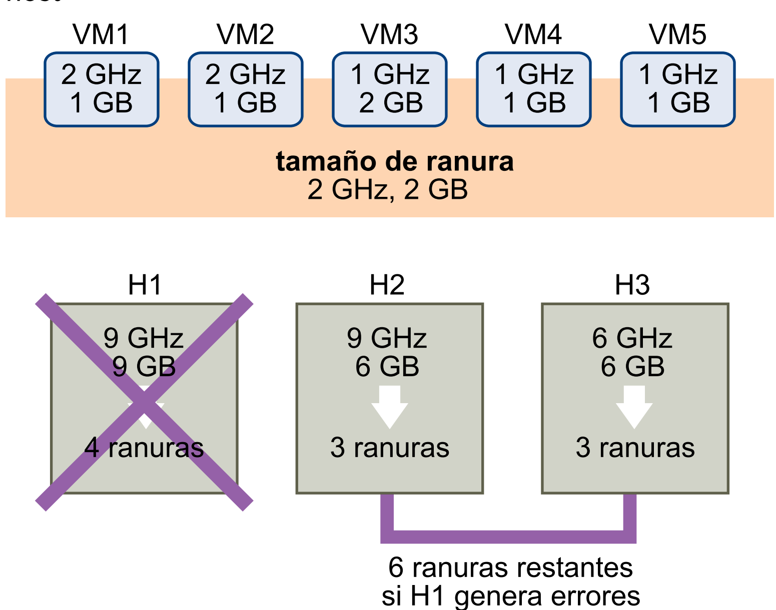
La capacidad actual de conmutación por error se calcula determinando cuántos hosts (comenzando desde el más grande) pueden generar errores y aún dejar suficientes ranuras para atender los requisitos de todas las máquinas virtuales encendidas.

Ejemplo: Control de admisión mediante la directiva de ranuras

La forma en que se calcula y se usa el tamaño de ranura con esta directiva de control de admisión se muestra en un ejemplo. Haga las siguientes suposiciones sobre un clúster:

- El clúster está compuesto de tres hosts, cada uno con una cantidad diferente de recursos de CPU y de memoria disponibles. El primer host (H1) posee 9 GHz de recursos de CPU disponibles y 9 GB de memoria disponible, en tanto que el host 2 (H2) tiene 9 GHz y 6 GB y el host 3 (H3) cuenta con 6 GHz y 6 GB.
- Existen cinco máquinas virtuales encendidas en el clúster con diferentes requisitos de CPU y memoria. La máquina virtual 1 necesita 2 GHz de recursos de CPU y 1 GB de memoria, en tanto que la máquina virtual 2 requiere 2 GHz y 1 GB, la máquina virtual 3, 1 GHz y 2 GB, la máquina virtual 4 necesita 1 GHz y 1 GB y la máquina virtual 5, 1 GHz y 1 GB.
- Tolerancias del clúster para errores del host está configurada en uno.

Figura 2-2. Ejemplo de control de admisión con directiva Tolerancias del clúster para errores del host



1 El tamaño de ranura se calcula comparando tanto los requisitos de CPU como de memoria de las máquinas virtuales y seleccionando el de mayor tamaño.

   El mayor requisito de CPU (compartido por la máquina virtual 1 y la máquina virtual 2) es 2 GHz, en tanto que el mayor requisito de memoria (para la máquina virtual 3) es 2 GB. Basado en esto, el tamaño de ranura es CPU de 2 GHz y memoria de 2 GB.

2 Se determina la cantidad máxima de ranuras que puede admitir cada host.

   H1 puede admitir cuatro ranuras. H2 puede admitir tres ranuras (que es la cantidad menor de 9 GHz/2 GHz y 6 GB/2 GB) y H3 también puede admitir tres ranuras.

3 Se calcula la capacidad actual de conmutación por error.

   El host más grande es el H1 y si genera errores, seis ranuras permanecen en el clúster, lo que es suficiente para las cinco máquinas virtuales encendidas. Si hay error tanto de H1 como de H2, solo quedan tres ranuras, lo que no es suficiente. Por lo tanto, la capacidad actual de conmutación por error es uno.

El clúster tiene una ranura disponible (las seis ranuras en H2 y H3 menos las cinco ranuras usadas).

Control de admisión de hosts de conmutación por error dedicados

Puede configurar vSphere HA para designar hosts específicos como hosts de conmutación por error.

Con el control de admisión de hosts de conmutación por error dedicados, cuando un host genera errores, vSphere HA intenta reiniciar sus máquinas virtuales en cualquiera de los hosts de conmutación por error especificados. Si esto no es posible, por ejemplo debido a que los hosts para conmutación por error presentaron errores o no tienen suficientes recursos, entonces vSphere HA intenta reiniciar aquellas máquinas virtuales en otros hosts en el clúster.

Para asegurar que haya capacidad disponible en un host para conmutación por error, se evita que encienda máquinas virtuales o use vMotion para migrar máquinas virtuales a un host para conmutación por error. Igualmente, DRS no usa un host para conmutación por error para equilibrio de carga.

Nota Si usa el control de admisión de hosts de conmutación por error dedicados y designa varios hosts de conmutación por error, DRS no intenta aplicar las reglas de afinidad Máquina virtual-Máquina virtual para máquinas virtuales que se están ejecutando en hosts de conmutación por error.

Interoperabilidad de vSphere HA

vSphere HA puede interoperar con muchas otras funciones, como DRS y vSAN.

Antes de configurar vSphere HA, se deben conocer las limitaciones de su interoperabilidad con estas otras funciones o productos.

Usar vSphere HA con vSAN

Puede usar vSAN como el almacenamiento compartido para un clúster de vSphere HA. Cuando se habilita, vSAN agrega los discos de almacenamiento local especificados a los hosts en un solo almacén de datos que comparten todos los hosts.

Para usar vSphere HA con vSAN, debe tener en cuenta ciertas consideraciones y limitaciones para la interoperabilidad de estas dos características.

Para obtener información sobre vSAN, consulte *Administrar VMware vSAN*.

Nota Puede usar vSphere HA con clústeres ampliados de vSAN.

Requisitos de los hosts ESXi

Puede usar vSAN con un clúster de vSphere HA solamente si se satisfacen las siguientes condiciones:

- Todos los hosts ESXi en el clúster deben ser de la versión 5.5 o posterior.
- El clúster debe tener un mínimo de tres hosts ESXi.

Diferencias de red

vSAN tiene su propia red. Si se habilitan vSAN y vSphere HA en el mismo clúster, el tráfico entre agentes de HA se transmite a través de esta red de almacenamiento en lugar de la red de administración. vSphere HA utiliza la red de administración únicamente si vSAN está deshabilitado. vCenter Server elige la red correcta si se configura vSphere HA en un host.

Nota Es posible habilitar vSAN únicamente si vSphere HA está deshabilitado.

Si cambia la configuración de red de vSAN, los agentes de vSphere HA no seleccionan de forma automática la nueva configuración de red. Para realizar cambios en la red de vSAN, debe llevar a cabo los siguientes pasos en vSphere Web Client:

1 Deshabilite Supervisión de hosts para el clúster de vSphere HA.

2 Efectúe los cambios en la red de vSAN.

3 Haga clic con el botón derecho en el clúster y seleccione **Volver a configurar para vSphere HA**.

4 Vuelva a habilitar Supervisión de hosts para el clúster de vSphere HA.

Tabla 2-2. Diferencias de red de vSphere HA muestra las diferencias en las redes vSphere HA, ya sea que se utilice vSAN o no.

Tabla 2-2. Diferencias de red de vSphere HA

	vSAN habilitado	vSAN deshabilitado
Red utilizada por vSphere HA	Red de almacenamiento de vSAN	Red de administración
Almacenes de datos de latidos	Cualquier almacén de datos montado en > 1 host, pero no almacenes de datos de vSAN	Cualquier almacén de datos montado en > 1 host
Host declarado aislado	No se puede hacer ping a las direcciones de aislamiento y la red de almacenamiento de vSAN no está accesible	No se puede hacer ping a las direcciones de aislamiento y la red de administración no está accesible

Configurar reserva de capacidad

Cuando reserva capacidad para su clúster de vSphere HA con una directiva de control de admisión, debe coordinar esta configuración con la configuración de vSAN correspondiente para garantizar la accesibilidad de datos cuando se produzcan errores. Específicamente, la configuración Número de errores que se toleran en el conjunto de reglas de vSAN no debe ser inferior a la capacidad que reserva la configuración de control de admisión de vSphere HA.

Por ejemplo, si el conjunto de reglas de vSAN solamente permite dos errores, la directiva de control de admisión de vSphere HA debe reservar una capacidad que sea equivalente a los errores de solamente un host o dos hosts. Si va a usar la directiva Porcentaje de recursos del clúster reservados para un clúster que tiene ocho hosts, no debe reservar más de un 25 % de los recursos del clúster. En el mismo clúster, con la directiva Tolerancias del clúster para errores del

host, la configuración no debe ser mayor a dos hosts. Si vSphere HA reserva menos capacidad, la actividad de conmutación por error puede ser impredecible. La reserva de capacidad en exceso restringe el encendido de las máquinas virtuales y las migraciones entre clústeres de vSphere vMotion.

Usar vSphere HA y DRS a la vez

El uso de vSphere HA con Distributed Resource Scheduler (DRS) combina la conmutación por error automática con el equilibrio de carga. Mediante esta combinación se puede obtener un clúster más equilibrado después de que vSphere HA haya movido máquinas virtuales a diferentes hosts.

Cuando vSphere HA realiza la conmutación por error y reinicia máquinas virtuales en hosts distintos, su principal prioridad es hacer que todas las máquinas virtuales estén disponibles de inmediato. Después de que se hayan reiniciado las máquinas virtuales, los hosts en los que estaban encendidas podrían verse con carga excesiva, mientras que otros hosts tienen en comparación una carga muy ligera. vSphere HA utiliza la reserva de CPU y memoria y la memoria de sobrecarga de la máquina virtual para determinar si un host tiene suficiente capacidad disponible para incluir la máquina virtual.

En un clúster que utiliza DRS y vSphere HA con control de admisión activado, es posible que las máquinas virtuales no se evacúen de los hosts que entran en modo de mantenimiento. Este comportamiento se produce debido a los recursos reservados para reiniciar máquinas virtuales en caso de un error. Debe migrar manualmente las máquinas virtuales de los hosts mediante el uso de vMotion.

En algunos casos, es posible que vSphere HA no pueda realizar la conmutación por error en máquinas virtuales debido a restricciones de recursos. Esto puede deberse a varios motivos.

- El control de admisión de HA está deshabilitado y Distributed Power Management (DPM) está habilitado. Esto puede provocar que DPM consolide máquinas virtuales en menor cantidad de hosts y que coloque los hosts vacíos en modo de espera, lo que no deja suficiente capacidad de encendido para realizar conmutación por error.
- Las reglas de afinidad Máquina virtual-Host (obligatorias) podrían limitar los hosts en los que se pueden colocar ciertas máquinas virtuales.
- Podría haber suficientes recursos totales, pero estos pueden fragmentarse en varios hosts con el fin de que las máquinas virtuales no puedan usarlos para la conmutación por error.

En dichos casos, vSphere HA puede utilizar DRS para intentar ajustar el clúster (por ejemplo, sacando los hosts del modo de espera o migrando máquinas virtuales para desfragmentar los recursos del clúster), de manera que HA pueda realizar las conmutaciones por error.

Si DPM está en modo manual, puede que tenga que confirmar las recomendaciones de encendido del host. Igualmente, si DRS está en modo manual, es posible que tenga que confirmar las recomendaciones de migración.

Si va a utilizar reglas de afinidad Máquina virtual-Host que son obligatorias, tenga en cuenta que estas no se pueden infringir. vSphere HA no realiza una conmutación por error si el hacerlo implica una infracción de una regla de este tipo.

Para obtener más información sobre DRS, consulte la documentación de *Administración de recursos de vSphere*.

Reglas de afinidad de vSphere HA y DRS

Si crea una regla de afinidad de DRS para su clúster, puede especificar de qué manera vSphere HA aplica esa regla durante la conmutación por error de una máquina virtual.

Los dos tipos de reglas para los cuales puede especificar comportamiento de conmutación por error de vSphere HA son los siguientes:

- Las reglas antiafinidad de la máquina virtual fuerzan a las máquinas virtuales especificadas para que permanezcan separadas durante las acciones de conmutación por error.
- Las reglas de afinidad Máquina virtual-Host colocan máquinas virtuales especificadas en un host particular o un miembro de un grupo definido de hosts durante acciones de conmutación por error.

Cuando se edita una regla de compatibilidad de DRS, se deben usar las opciones avanzadas de vSphere HA para aplicar el comportamiento de conmutación por error deseado a vSphere HA.

- **HA debe respetar las reglas de antiafinidad de máquina virtual durante la conmutación por error** -- Cuando se establece la opción avanzada para las reglas de antiafinidad de máquina virtual, vSphere HA no conmuta por error en una máquina virtual si ello infringe una regla. En su lugar, vSphere HA emite un evento que indica que no hay suficientes recursos para realizar la conmutación por error.
- **HA debe respetar las reglas de afinidad máquina virtual a host durante la conmutación por error**: si es posible, vSphere HA intenta poner las máquina virtual con esta regla en los hosts especificados.

Para obtener más información, consulte las opciones avanzadas de vSphere HA.

Nota vSphere HA puede reiniciar una máquina virtual en un clúster con DRS deshabilitado, con lo que se anula una asignación de reglas de afinidad Máquina virtual-Host si el error del host se produce poco después de configurar la regla (de forma predeterminada, en 5 minutos).

Otros problemas de interoperabilidad de vSphere HA

Para usar vSphere HA, debe tener en cuenta los siguientes problemas de interoperabilidad adicionales.

Protección de componentes de la máquina virtual

Protección de componentes de la máquina virtual (VMCP) tiene los siguientes problemas y limitaciones de interoperabilidad:

- VMCP no es compatible con vSphere Fault Tolerance. Si VMCP se habilita para un clúster mediante Fault Tolerance, las máquinas virtuales con FT afectadas recibirán automáticamente anulaciones que deshabilitan VMCP.
- VMCP no detecta ni responde a problemas de accesibilidad para archivos localizados en almacenes de datos de vSAN. Si los archivos de configuración y VMDK de una máquina virtual están situados solo en almacenes de datos de vSAN, no cuentan con protección de VMCP.
- VMCP no detecta ni responde a problemas de accesibilidad para archivos localizados en almacenes de datos de Virtual Volumes. Si los archivos de configuración y VMDK de una máquina virtual están situados solo en almacenes de datos de Virtual Volumes no cuentan con protección de VMCP.
- VMCP no protege contra asignación de dispositivos sin formato (RDM) inaccesible.

IPv6

vSphere HA se puede usar con configuraciones de red IPv6, que son plenamente compatibles si se cumplen las siguientes consideraciones:

- El clúster contiene solo hosts ESXi 6.0 o versiones posteriores.
- La red de administración para todos los hosts en el clúster debe configurarse con la misma versión de IP, ya sea IPv6 o IPv4. Los clústeres de vSphere HA no pueden contener ambos tipos de configuración de redes.
- Las direcciones de aislamiento de red que usa vSphere HA deben coincidir con la versión IP que utiliza el clúster para su red de administración.
- IPv6 no se puede usar en clústeres de vSphere HA que también emplean vSAN.

Además de las restricciones anteriores, tampoco se admite el uso de los siguientes tipos de direcciones IPv6 con la red de administración o la dirección de aislamiento de vSphere HA : dirección local de vínculo, ORCHID y dirección local de vínculo con índices de zona. Igualmente, el tipo de dirección de bucle invertido no se puede usar para la red de administración.

Nota Para actualizar una implementación existente de IPv4 a IPv6, primero debe deshabilitar vSphere HA.

Crear un clúster de vSphere HA

vSphere HA opera en el contexto de un clúster de hosts ESXi (o ESX heredado). Debe crear un clúster, rellenarlo con hosts y configurar los parámetros de vSphere HA antes de que pueda establecerse la protección de conmutación por error.

Cuando cree un clúster de vSphere HA, deberá configurar varios parámetros que determinan la manera en que funciona la característica. Antes de hacerlo, identifique los nodos del clúster. Estos nodos son los hosts ESXi que proporcionarán los recursos para admitir máquinas virtuales y que vSphere HA usará para la protección de conmutación por error. Después deberá determinar de qué forma se conectarán estos nodos entre sí y con el almacenamiento compartido donde se encuentran los datos de su máquina virtual. Después de que se instale esa arquitectura de redes, puede agregar los hosts al clúster y concluir la configuración de vSphere HA.

Puede habilitar y configurar vSphere HA antes de agregar nodos de hosts al clúster. Sin embargo, hasta que se agreguen los hosts, su clúster no estará totalmente operativo y parte de la configuración del clúster no estará disponible. Por ejemplo, la directiva de control de admisión Especificar hosts para conmutación por error no está disponible hasta que haya un host que pueda designarse como el host para conmutación por error.

Nota La característica Inicio y apagado de máquina virtual (inicio automático) está deshabilitada para todas las máquinas virtuales que residen en hosts que se encuentran en (o se agregan a) un clúster de vSphere HA. El inicio automático no se admite cuando se utiliza con vSphere HA.

Lista de comprobación de vSphere HA

La lista de comprobación de vSphere HA contiene requisitos que debe tener en cuenta antes de crear y utilizar un clúster de vSphere HA.

Repase esta lista antes de configurar un clúster de vSphere HA. Para obtener más información, siga la referencia adecuada.

- Todos los hosts deben tener licencias para vSphere HA.
- Un clúster debe contener al menos dos hosts.
- Todos los hosts deben estar configurados con direcciones IP estáticas. Si utiliza DHCP, debe asegurarse de que la dirección de cada host se mantiene después de los reinicios.
- Todos los hosts deben tener al menos una red de administración en común. La práctica recomendada es tener al menos dos redes de administración en común. Debe utilizar la red VMkernel con la casilla **Management traffic** (Tráfico de administración) habilitada. En las redes de administración, las redes deben poder accederse mutuamente, lo mismo que vCenter Server y los hosts. Consulte Prácticas recomendadas para redes.
- Para asegurarse de que cualquier máquina virtual pueda ejecutarse en cualquier host en el clúster, todos los hosts deben tener acceso a las mismas redes y almacenes de datos de las máquinas virtuales. De manera similar, las máquinas virtuales deben estar ubicadas en el almacenamiento compartido, no local. De lo contrario, no podrán realizar conmutación por error en caso de un error en el host.

  Nota vSphere HA utiliza latidos del almacén de datos para distinguir entre hosts particionados, aislados y con errores. Por lo tanto, si algunos almacenes de datos son más confiables en el entorno, configure vSphere HA para que les otorgue preferencia.

- Para que la supervisión de máquina virtual funcione, VMware Tools debe estar instalado. Consulte Supervisar máquina virtual y aplicaciones.
- vSphere HA es compatible con IPv4 e IPv6. Consulte Otros problemas de interoperabilidad de vSphere HA para ver las consideraciones cuando use IPv6.
- Para que VM Component Protection (Protección de componentes de la máquina virtual) funcione, los hosts deben tener la característica de tiempo de espera de todas las rutas de acceso inactivas (All Paths Down, APD) habilitada.
- Para utilizar VM Component Protection (Protección de componentes de la máquina virtual), los clústeres deben contener hosts ESXi 6.0 o posteriores.
- Solo los clústeres de vSphere HA que contengan hosts ESXi 6.0 o posteriores pueden utilizarse para habilitar VMCP. Los clústeres que contienen hosts de una versión anterior no pueden habilitar VMCP y esos hosts no pueden agregarse a un clúster habilitado para VMCP.
- Si su clúster utiliza almacenes de datos de Virtual Volume, cuando vSphere HA está habilitado, vCenter Server crea Virtual Volume de configuración en cada almacén de datos. En estos contenedores, vSphere HA almacena los archivos que utiliza para proteger las máquinas virtuales. vSphere HA no funciona correctamente si elimina estos contenedores. Solo se crea un contenedor por almacén de datos de Virtual Volume.

Crear un clúster de vSphere HA

Para habilitar su clúster para vSphere HA, primero debe crear un clúster vacío. Después de planificar los recursos y la arquitectura de redes de su clúster, use vSphere Web Client para agregar hosts al clúster y especificar la configuración de vSphere HA del clúster.

Disponer de un clúster habilitado para vSphere HA es un requisito previo para vSphere Fault Tolerance.

Requisitos previos

- Compruebe que todas las máquinas virtuales y sus archivos de configuración residan en el almacenamiento compartido.
- Compruebe que los hosts estén configurados para acceder al almacenamiento compartido, de manera que pueda encender las máquinas virtuales utilizando diferentes hosts en el clúster.
- Compruebe que los hosts estén configurados para tener acceso a la red de máquina virtual.
- Compruebe que está usando conexiones de red de administración redundantes para vSphere HA. Para obtener información acerca de cómo configurar la redundancia de la red, consulte Prácticas recomendadas para redes.
- Compruebe que ha configurado hosts con al menos dos almacenes de datos para ofrecer redundancia para la verificación de latidos del almacén de datos de vSphere HA.
- Conecte vSphere Web Client a vCenter Server utilizando una cuenta con permisos de administrador de clúster.

Procedimiento

1. En vSphere Web Client, desplácese hasta el centro de datos donde desea que resida el clúster y haga clic en **Crear un clúster**.
2. Complete el asistente **Clúster nuevo**.

   No active vSphere HA (o DRS).
3. Haga clic en **Aceptar** para cerrar el asistente y crear un clúster vacío.
4. Según su plan para los recursos y la arquitectura de redes del clúster, use vSphere Web Client para agregar hosts al clúster.
5. Desplácese hasta el clúster y habilite vSphere HA.
   a. Haga clic en la pestaña **Configurar**.
   b. Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.
   c. Seleccione **Activar vSphere HA**.
   d. Seleccione **Activar Proactive HA** para permitir migraciones proactivas de máquinas virtuales desde hosts en los cuales el host notificó una degradación de estado.
6. En **Errores y respuestas**, seleccione **Habilitar supervisión de hosts**.

   Con la opción Supervisión de hosts habilitada, los hosts del clúster pueden intercambiar latidos de red y vSphere HA puede tomar medidas cuando detecta errores. La función de supervisión de host es necesaria para que el proceso de recuperación de vSphere Fault Tolerance funcione correctamente.
7. Seleccione una configuración para **Supervisión de máquinas virtuales**.

   Seleccione **Solo supervisión de máquina virtual** para reiniciar las máquinas virtuales individuales que no emitieron latidos por un tiempo determinado. También puede seleccionar **Supervisión de máquina virtual y aplicaciones** para habilitar la supervisión de aplicaciones.
8. Haga clic en **Aceptar**.

Resultados

Tiene un clúster de vSphere HA lleno de hosts.

Pasos siguientes

Configure los parámetros de vSphere HA adecuados para su clúster.

- Errores y respuestas
- Errores y respuestas de Proactive HA
- Control de admisión
- Almacenes de datos de latidos
- Opciones avanzadas

Consulte Configurar los parámetros de disponibilidad de vSphere.

Configurar los parámetros de disponibilidad de vSphere

Cuando se crea un clúster vSphere HA o se configura un clúster existente, se debe ajustar la configuración que determina cómo funciona la característica.

En vSphere Web Client, puede establecer la siguiente configuración de vSphere HA:

Errores y respuestas

Proporcione aquí la configuración para respuestas de error de host, aislamiento de host, supervisión de máquinas virtuales y Protección de componentes de la máquina virtual.

Errores y respuestas de Proactive HA

Introduzca la configuración para indicar de qué forma debe responder Proactive HA cuando un proveedor notifica una degradación de estado a vCenter, lo que indica un error parcial de ese host.

Control de admisión

Habilite o deshabilite el control de admisión del clúster vSphere HA y elija una directiva para la manera en que se aplicará.

Almacenes de datos de latidos

Especifique las preferencias de los almacenes de datos que utiliza vSphere HA para los latidos de almacén de datos.

Opciones avanzadas

Personalice el comportamiento de vSphere HA configurando las opciones avanzadas.

Configurar respuestas a errores

El panel **Error y respuestas** de la configuración de vSphere HA permite configurar cómo debe funcionar el clúster cuando se encuentran problemas.

En esta parte de vSphere Web Client, se pueden determinar las respuestas específicas del clúster de vSphere HA para el aislamiento y los errores de host. También se pueden configurar las acciones de VMCP para las situaciones de pérdida permanente de dispositivos (Permanent Device Loss, PDL) y de inactividad de todas las rutas de acceso (All Paths Down, APD), y se puede habilitar la supervisión de máquinas virtuales.

Las siguientes tareas están disponibles:

Procedimiento

1 Responder a error de host

Puede configurar respuestas específicas a errores de host que se produzcan en el clúster de vSphere HA.

2 Responder a aislamiento de host

Puede configurar respuestas específicas a aislamientos de host que se produzcan en el clúster de vSphere HA.

3 Configurar respuestas de VMCP

Configure la respuesta que tendrá Protección de componentes de la máquina virtual (VM Component Protection, VMCP) cuando un almacén de datos encuentre un error de PDL o APD.

4 Habilitar supervisión de máquinas virtuales

Se puede activar la supervisión de máquinas virtuales y aplicaciones y, además, establecer la sensibilidad de la supervisión para el clúster de vSphere HA.

Responder a error de host

Puede configurar respuestas específicas a errores de host que se produzcan en el clúster de vSphere HA.

Esta página solo se puede editar si se habilitó vSphere HA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Haga clic en **Errores y respuestas** y expanda **Respuesta de error de host**.

5 Seleccione una de las siguientes opciones de configuración.

Opción	Descripción
Respuesta de error	Si se selecciona **Deshabilitado**, esta configuración desactiva la supervisión del host y las máquinas virtuales no se reinician cuando se producen errores de host. Si se selecciona **Reiniciar las máquinas virtuales**, las máquinas virtuales se someten a conmutación por error según su prioridad de reinicio cuando se produce un error de host.
Prioridad de reinicio de máquina virtual predeterminada	La prioridad de reinicio determina el orden en el que se reinician las máquinas virtuales cuando el host falla. Las máquinas virtuales con mayor prioridad se inician primero. Si varios hosts fallan, todas las máquinas virtuales se migran del primer host en el orden de prioridad, después se migran todas las máquinas virtuales del segundo host en el orden de prioridad, etc.
Condición de reinicio de dependencia de máquina virtual	Se debe seleccionar una condición específica, así como un retraso, después de que se haya cumplido la condición, para que vSphere HA pueda continuar con la siguiente prioridad de reinicio de máquina virtual.

6 Haga clic en **Aceptar**.

Resultados

Se aplica la configuración para la respuesta al error de host.

Responder a aislamiento de host

Puede configurar respuestas específicas a aislamientos de host que se produzcan en el clúster de vSphere HA.

Esta página solo se puede editar si se habilitó vSphere HA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Haga clic en **Errores y respuestas** y expanda **Respuesta para el aislamiento del host**.

5 Para configurar la respuesta de aislamiento del host, seleccione **Deshabilitado**, **Desconectar y reiniciar las máquinas virtuales** o **Apagar y reiniciar las máquinas virtuales**.

6 Haga clic en **Aceptar**.

Resultados

Se aplica la configuración para la respuesta al aislamiento de host.

Configurar respuestas de VMCP

Configure la respuesta que tendrá Protección de componentes de la máquina virtual (VM Component Protection, VMCP) cuando un almacén de datos encuentre un error de PDL o APD.

Esta página solo se puede editar si se habilitó vSphere HA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Haga clic en **Errores y respuestas** y expanda **Almacén de datos con PDL** o **Almacén de datos con APD**.

5 Si hizo clic en **Almacén de datos con PDL**, puede establecer la respuesta de error de VMCP para este tipo de problema, ya sea **Deshabilitado**, **Emitir eventos** o **Apagar y reiniciar las máquinas virtuales**.

6 Si hizo clic en **Almacén de datos con APD**, puede establecer la respuesta de error de VMCP para este tipo de problema, ya sea **Deshabilitado**, **Emitir eventos**, **Apagar y las reiniciar máquinas virtuales--Directiva de reinicio conservadora** o **Apagar y las reiniciar las máquinas virtuales--Directiva de reinicio agresiva**. También puede establecer la opción **Recuperación de respuesta**, que es la cantidad de minutos que VMCP espera antes de realizar una acción.

7 Haga clic en **Aceptar**.

Resultados

Se aplica la configuración para la respuesta de error de VMCP.

Habilitar supervisión de máquinas virtuales

Se puede activar la supervisión de máquinas virtuales y aplicaciones y, además, establecer la sensibilidad de la supervisión para el clúster de vSphere HA.

Esta página solo se puede editar si se habilitó vSphere HA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Haga clic en **Errores y respuestas** y expanda **Supervisión de máquinas virtuales**.

5 Seleccione **Supervisión de máquinas virtuales** y **Supervisión de aplicaciones**.

   Estas opciones activan los latidos de VMware Tools y de la aplicación, respectivamente.

6 Para configurar la sensibilidad de supervisión de los latidos, mueva el control deslizante entre **Bajo** y **Alto** o seleccione **Personalizar** para proporcionar parámetros personalizados.

7 Haga clic en **Aceptar**.

Resultados

Se aplica la configuración de supervisión.

Configurar Proactive HA

Se puede configurar la forma en que responde Proactive HA cuando un proveedor notifica su degradación de estado a vCenter, lo que indica un error parcial de ese host.

Esta página se puede editar únicamente si se habilitó vSphere DRS.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de Proactive HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Seleccione **Activar Proactive HA**.

5 Haga clic en **Errores y respuestas de Proactive HA**.

6 Seleccione una de las siguientes opciones de configuración.

Opción	Descripción
Nivel de automatización	Determine si el modo de cuarentena o de mantenimiento de host y las migraciones de máquina virtual son recomendaciones o avisos automáticos. ■ **Manual**. vCenter Server sugiere recomendaciones de migración para las máquinas virtuales. ■ **Automático**. Las máquinas virtuales se migran a hosts en un estado correcto y los hosts degradados se ponen en cuarentena o en modo de mantenimiento según el nivel de automatización de Proactive HA configurado.
Corrección	Determine qué sucede con los hosts parcialmente degradados. ■ **Modo de cuarentena para todos los errores**. Equilibra el rendimiento y la disponibilidad; para ello, evita usar los hosts parcialmente degradados siempre que el rendimiento de las máquinas virtuales no se vea afectado. ■ **Modo de cuarentena para modo moderado y de mantenimiento para errores graves (mixto)**. Equilibra el rendimiento y la disponibilidad; para ello, evita usar los hosts moderadamente degradados siempre que el rendimiento de las máquinas virtuales no se vea afectado. Garantiza que las máquinas virtuales no se ejecuten en hosts con errores graves. ■ **Modo de mantenimiento para todos los errores**. Garantiza que las máquinas virtuales no se ejecuten en hosts con errores parciales. Se requieren privilegios de `Host.Config.Quarantine` y `Host.Config.Maintenance` para colocar los hosts en modo de cuarentena y modo de mantenimiento, respectivamente.

Para habilitar proveedores de Proactive HA en este clúster, seleccione las casillas. Los proveedores aparecen una vez que se instaló el complemento de vSphere Web Client correspondiente y supervisan todos los hosts del clúster. Para ver o editar las condiciones de error que admite el proveedor, haga clic en el vínculo de edición.

7 Haga clic en **Aceptar**.

Configurar el control de admisión

Después de crear un clúster, se puede configurar el control de admisión para especificar si se pueden iniciar las máquinas virtuales que infringen restricciones de disponibilidad. El clúster reserva recursos para que se pueda llevar a cabo la conmutación por error de todas las máquinas virtuales en ejecución en la cantidad de hosts especificada.

La página Control de admisión aparece solo si ha habilitado vSphere HA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Haga clic en **Control de admisión** para visualizar las opciones de configuración.

5 Seleccione un número para **Errores del host que tolera el clúster**. Esta es la cantidad máxima de errores del host para la que el clúster puede garantizar su recuperación o la conmutación por error.

6 Seleccione una opción para **Definir capacidad de conmutación por error del host por**.

Opción	Descripción
Porcentaje de recursos del clúster	Especifique un porcentaje de los recursos de memoria y CPU del clúster que desea reservar como capacidad disponible para admitir las conmutaciones por error.
Directiva de ranura (máquinas virtuales encendidas)	Seleccione una directiva de tamaño de ranura que cubra todas las máquinas virtuales encendidas o que especifique un tamaño fijo. También puede calcular cuántas máquinas virtuales requieren varias ranuras.
Hosts de conmutación por error dedicados	Seleccione los hosts que vaya a utilizar para las acciones de conmutación por error. Las conmutaciones por error se pueden producir en otros hosts en el clúster si un host de conmutación por error predeterminado no tiene suficientes recursos.
Deshabilitado	Seleccione esta opción para deshabilitar el control de admisión y permitir el encendido de máquinas virtuales que infrinjan restricciones de disponibilidad.

7 Establezca el porcentaje para la opción **Degradación del rendimiento que toleran las máquinas virtuales**.

Esta opción determina qué porcentaje de degradación de rendimiento pueden tolerar las máquinas virtuales en el clúster durante un error.

8 Haga clic en **Aceptar**.

Resultados

Se aplica la configuración del control de admisión.

Configurar almacenes de datos de latidos

vSphere HA utiliza latidos de almacén de datos para distinguir entre los hosts con errores y los hosts que residen en una partición de red. Con los latidos de almacén de datos, vSphere HA puede supervisar los hosts cuando se produce la partición de una red de administración y seguir respondiendo ante los errores.

Puede especificar los almacenes de datos que desea que se utilicen para verificar el latido del almacén de datos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Haga clic en **Almacenes de datos de latidos** para visualizar las opciones de configuración de latidos de almacén de datos.

5 Para proporcionar instrucciones a vSphere HA acerca de cómo seleccionar los almacenes de datos y la manera de tratar las preferencias, seleccione entre las siguientes opciones.

Tabla 2-3.

Opciones de latidos de almacén de datos
Seleccionar automáticamente almacenes de datos accesibles desde el host
Utilizar almacenes de datos solo desde la lista especificada
Utilizar almacenes de datos desde la lista y el complemento especificados automáticamente si es necesario

6 En el panel Almacenes de datos de latidos disponibles, seleccione los almacenes de datos que desea usar para latidos.

Los almacenes de datos que figuran son los compartidos por más de un host en el clúster de vSphere HA. Cuando se selecciona un almacén de datos, el panel inferior muestra todos los hosts en el clúster vSphere HA que pueden acceder a él.

7 Haga clic en **Aceptar**.

Configurar opciones avanzadas

Para personalizar el comportamiento de vSphere HA, configure las opciones avanzadas de vSphere HA.

Requisitos previos

Compruebe que dispone de privilegios de administrador del clúster.

Nota Debido a que estas opciones afectan el funcionamiento de vSphere HA, cámbielas con precaución.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 Seleccione **Disponibilidad de vSphere** y haga clic en **Editar**.

4 Haga clic en **Opciones avanzadas**.

5 Haga clic en **Agregar** y escriba el nombre de la opción avanzada en el cuadro de texto.

Puede configurar el valor de la opción en el cuadro de texto de la columna Valor.

6 Repita el paso 5 para cada nueva opción que desee agregar y haga clic en **Aceptar**.

Resultados

El clúster utiliza las opciones que haya agregado o modificado.

Pasos siguientes

Una vez que haya configurado una opción avanzada de vSphere HA, se mantendrá hasta que realice una de estas acciones:

- Utilizar vSphere Web Client para restablecer el valor predeterminado.
- Editar o eliminar manualmente la opción del archivo fdm.cfg en todos los hosts del clúster.

Opciones avanzadas de vSphere HA

Puede configurar opciones avanzadas que influyen en el comportamiento del clúster de vSphere HA.

Tabla 2-4. Opciones avanzadas de vSphere HA

Opción	Descripción
`das.isolationaddress[...]`	Determina la dirección a la que se hará ping con el fin de determinar si un host está aislado de la red. Se hace ping a esta dirección solo cuando no se reciben latidos de ningún otro host en el clúster. Si no se especifica, se usa la puerta de enlace predeterminada de la red de administración. Esta puerta de enlace predeterminada tiene que ser una dirección confiable que esté disponible, de manera que el host pueda determina si está aislado de la red. Puede especificar varias direcciones de aislamiento para el clúster (hasta 10): `das.isolationAddressX`, donde X = 0-9. Comúnmente, se recomienda especificar una por red de administración. Si se especifican demasiadas direcciones, la detección de aislamiento tarda demasiado.
`das.usedefaultisolationaddress`	De forma predeterminada, vSphere HA utiliza como dirección de aislamiento la puerta de enlace predeterminada de la red de consola. Esta opción especifica si se usa o no esta puerta de enlace predeterminada (true|false).
`das.isolationshutdowntimeout`	El período que espera el sistema para que se desconecte una máquina virtual antes de apagarla. Esto solo se aplica si la respuesta de aislamiento del host es Apagar máquina virtual. El valor predeterminado es 300 segundos.
`das.slotmeminmb`	Define el límite máximo del tamaño de ranura de memoria. Si se utiliza esta opción, el tamaño de ranura es el menor valor de este o la reserva de memoria máxima más la sobrecarga de memoria de cualquier máquina virtual encendida en el clúster.
`das.slotcpuinmhz`	Define el límite máximo del tamaño de ranura de CPU. Si se utiliza esta opción, el tamaño de ranura es el menor valor de este o la reserva de CPU máxima de cualquier máquina virtual encendida en el clúster.

Tabla 2-4. Opciones avanzadas de vSphere HA (continuación)

Opción	Descripción
das.vmmemoryminmb	Define el valor de recurso de memoria predeterminado asignado a una máquina virtual en caso de que su reserva de memoria no esté especificada o sea cero. Esto se usa para la directiva de control de admisión Tolerancias del clúster para errores del host. Si no se especifica ninguno, el valor predeterminado es 0 MB.
das.vmcpuminmhz	Define el valor de recurso de CPU predeterminado asignado a una máquina virtual en caso de que su reserva de CPU no esté especificada o sea cero. Esto se usa para la directiva de control de admisión Tolerancias del clúster para errores del host. Si no se especifica ninguno, el valor predeterminado es 32 MHz.
das.iostatsinterval	Cambia el intervalo de estadísticas de E/S predeterminado para sensibilidad de supervisión de la máquina virtual. El valor predeterminado es 120 (segundos). Puede configurarse para cualquier valor igual o superior a 0. Si se configura en 0 se desactiva la comprobación. **Nota** No se recomiendan valores inferiores a 50, ya que los valores menores pueden hacer que vSphere HA restablezca de forma inesperada una máquina virtual.
das.ignoreinsufficienthbdatastore	Desactiva problemas de configuración que se crean si el host no tiene suficientes almacenes de datos de latidos para vSphere HA. El valor predeterminado es false.
das.heartbeatdsperhost	Cambia la cantidad de almacenes de datos de latidos que se requieren. Los valores válidos pueden ir entre 2-5 y el valor predeterminado es 2.
das.config.fdm.isolationPolicyDelaySec	La cantidad de segundos que espera el sistema antes de ejecutar la directiva de aislamiento una vez que se determina que un host está aislado. El valor mínimo es 30. Si se configura en un valor menor a 30, el retraso será de 30 segundos.
das.respectvmvmantiaffinityrules	Determina si vSphere HA aplica las reglas de antiafinidad entre máquinas virtuales. El valor predeterminado es "true" y las reglas se aplican aunque vSphere DRS no esté habilitado. En este caso, vSphere HA no realiza conmutación por error en una máquina virtual si ello infringe una regla, pero sí emite un evento que indica que no hay suficientes recursos para ejecutar la conmutación por error. También se puede establecer esta opción en "false", con lo cual no se aplican las reglas. Consulte *Administración de recursos de vSphere* para obtener más información sobre reglas de antiafinidad.
das.maxresets	La cantidad máxima de intentos de restablecimiento que hace VMCP. Si se produce un error en una operación de restablecimiento en una máquina virtual afectada por una situación de APD, VMCP reintenta el restablecimiento esta cantidad de veces antes de rendirse.

Tabla 2-4. Opciones avanzadas de vSphere HA (continuación)

Opción	Descripción
`das.maxterminates`	La cantidad máxima de reintentos que hace VMCP para finalización de máquinas virtuales.
`das.terminateretryintervalsec`	Si VMCP no finaliza una máquina virtual, esta es la cantidad de segundos que espera el sistema antes de que reintente un intento de finalización.
`das.config.fdm.reportfailoverfailevent`	Cuando está configurado en 1, habilita la generación de un evento por máquina virtual detallado cuando un intento por parte de vSphere HA para reiniciar una máquina virtual no resulte correcto. El valor predeterminado es 0. En versiones anteriores a vSphere 6.0, este evento se genera de forma predeterminada.
`vpxd.das.completemetadataupdateintervalsec`	El período (en segundos) después de que se establece una regla de afinidad Máquina virtual-Host durante el cual vSphere HA puede reiniciar una máquina virtual en un clúster de DRS deshabilitado, con lo que se anula la regla. El valor predeterminado es 300 segundos.
`das.config.fdm.memReservationMB`	De forma predeterminada, los agentes de vSphere HA se ejecutan con un límite de memoria configurado de 250 MB. Puede que un host no permita esta reserva si se ejecuta fuera de la capacidad reservable. Puede usar esta opción avanzada para disminuir el límite de memoria a fin de evitar este problema. Solo es posible especificar números enteros mayores de 100, que es el valor mínimo. Al contrario, para evitar problemas durante las elecciones del agente principal en un clúster grande (que contiene de 6000 a 8000 máquinas virtuales), debe elevar este límite a 325 MB. **Nota** Una vez que se cambia este límite, debe ejecutar la tarea Volver a configurar alta disponibilidad para todos los hosts en el clúster. Igualmente, cuando se agrega un nuevo host al clúster o se reinicia el host existente, esta tarea debe realizarse en estos hosts a fin de actualizar esta configuración de memoria.

Tabla 2-4. Opciones avanzadas de vSphere HA (continuación)

Opción	Descripción
das.reregisterrestartdisabledvms	Cuando se deshabilita vSphere HA en una máquina virtual específica, esta opción garantiza que la máquina virtual se registre en otro host después de un error. Esto permite encender esa máquina virtual sin tener que volver a registrarla manualmente. **Nota** Cuando se utiliza esta opción, vSphere HA no enciende la máquina virtual, sino que la registra.
das.respectvmhostsoftaffinityrules	Determina si vSphere HA debe reiniciar una máquina virtual correspondiente en un host que pertenece al mismo grupo de máquina virtual-host. Si no existe un host con esas características o si el valor de esta opción se establece en "false", vSphere HA reinicia la máquina virtual en cualquier host disponible en el clúster. En vSphere 6.5, el valor predeterminado es "true". Es posible que este valor no esté visiblemente definido en las opciones avanzadas de HA del clúster. Si desea deshabilitar la opción, debe establecer manualmente esta opción en "false" en las opciones avanzadas de HA del clúster.

Nota Si cambia el valor de cualquiera de las siguientes opciones avanzadas, debe deshabilitar y volver a habilitar vSphere HA para que sus cambios surtan efecto.

- das.isolationaddress[...]
- das.usedefaultisolationaddress
- das.isolationshutdowntimeout

Personalizar una máquina virtual individual

Cada máquina virtual en un clúster de vSphere HA tiene asignada la configuración predeterminada del clúster para Prioridad de reinicio de máquinas virtuales, Respuesta de aislamiento del host, Protección de componentes de la máquina virtual y Supervisión de máquinas virtuales. Si se cambian estos valores predeterminados se puede definir el comportamiento específico de cada máquina virtual. Si la máquina virtual sale del clúster, esta configuración se pierde.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Configurar**.

3 En Configuración, seleccione **Reemplazos de máquina virtual** y haga clic en **Agregar**.

4 Use el botón **+** para seleccionar máquinas virtuales a las cuales aplicar los reemplazos.

5 Haga clic en **Aceptar**.

6 (opcional) Puede cambiar otras opciones de configuración, como **Nivel automático**, **Prioridad de reinicio de máquinas virtuales**, **Respuesta para aislamiento de host**, Configuración de VMCP, **Supervisión de máquinas virtuales** o **Sensibilidad de la supervisión de las máquinas virtuales**.

Nota Puede ver los valores predeterminados del clúster para esta configuración expandiendo primero **Configuración relevante del clúster** y luego ampliando **vSphere HA**.

7 Haga clic en **Aceptar**.

Resultados

Ahora el comportamiento de la máquina virtual se diferencia de los valores predeterminados del clúster para cada configuración que cambió.

Prácticas recomendadas para clústeres de VMware vSphere® High Availability

Para asegurar un rendimiento óptimo del clúster de vSphere HA, se deben seguir ciertas prácticas recomendadas. En esta sección se destacan algunas de las prácticas recomendadas clave para un clúster de vSphere HA.

También puede consultar la publicación *Prácticas recomendadas para la implementación de vSphere High Availability* para ver un análisis más detallado.

Prácticas recomendadas para redes

Siga las siguientes prácticas recomendadas para la configuración de NIC de host y topología de red para vSphere HA. Las prácticas recomendadas incluyen recomendaciones para los hosts ESXi, y para cableado, conmutadores, enrutadores y firewalls.

Configurar y realizar mantenimiento a la red

Las siguientes sugerencias de mantenimiento de la red pueden ayudarle a evitar la detección accidental de host con error y aislamiento de la red debido a baja de latidos de vSphere HA.

- Cuando se hacen cambios en las redes donde se encuentran sus hosts ESXi en clúster, suspenda la función Supervisión de hosts. Si cambia su configuración de hardware de red o de redes, se pueden interrumpir los latidos que vSphere HA usa para detectar errores de host; esto podría dar como resultado intentos no deseados de realizar conmutación por error en las máquinas virtuales.

- Cuando cambia la configuración de redes en los hosts mismos de ESXi, por ejemplo, agregando grupos de puertos o quitando vSwitches, suspenda Supervisión de hosts. Después de que haya hecho los cambios de configuración de redes, debe volver a configurar vSphere HA en todos los hosts en el clúster, lo que hace que se vuelva a inspeccionar la información de la red. Luego vuelva a habilitar Supervisión de hosts.

Nota Debido a que las redes son un componente vital de vSphere HA, si se debe realiza mantenimiento de red, informe al administrador de vSphere HA.

Redes usadas para comunicaciones de vSphere HA

Para identificar cuáles operaciones de red podrían interrumpir el funcionamiento de vSphere HA, debe saber cuáles redes de administración se están usando para la determinación de latidos y otras comunicaciones de vSphere HA.

- En hosts ESX heredados en el clúster, las comunicaciones de vSphere HA pasan por todas las redes que están designadas como redes de consola de servicio. Estos hosts no usan redes de VMkernel para comunicaciones de vSphere HA. Para contener el tráfico de vSphere HA a un subconjunto de las redes de consola de ESX, use la opción avanzada `allowedNetworks`.
- En hosts ESXi en el clúster, las comunicaciones de vSphere HA pasan de forma predeterminada por redes de VMkernel. Con un host ESXi, si desea usar una red diferente a la que utiliza vCenter Server para comunicarse con el host para vSphere HA, debe habilitar explícitamente la casilla **Tráfico de administración**.

Para mantener el tráfico de agente de vSphere HA en las redes que especificó, configure los hosts para que los vmkNIC utilizados por vSphere HA no comparten las subredes con los vmkNIC que emplea para otros fines. Los agentes de vSphere HA envían paquetes con cualquier pNIC que está asociado con una subred determinada cuando también hay al menos un vmkNIC configurado para el tráfico de administración de vSphere HA. Por lo tanto, para asegurar la separación de flujos de redes, los vmkNIC que emplean vSphere HA y otras funciones deben estar en subredes diferentes.

Direcciones de aislamiento de la red

Una dirección de aislamiento de la red es una dirección IP a la que se hace ping para determinar si un host está aislado de la red. Se hace ping a esta dirección solo cuando un host ha dejado de recibir latidos de todos los otros hosts en el clúster. Si un host puede hacer ping a su dirección de aislamiento de la red, el host no está aislado de la red y los otros hosts en el clúster han generado errores o están con partición de red. Sin embargo, si el host no puede hacer ping a su dirección de aislamiento, es probable que el host se haya aislado de la red y que no se tome una acción de conmutación por error.

De forma predeterminada, la dirección de aislamiento de la red es la puerta de enlace predeterminada para el host. Solo se especifica una puerta de enlace predeterminada, independientemente de cuántas redes de administración se hayan definido. Debe usar la opción avanzada `das.isolationaddress[...]` para agregar direcciones de aislamiento para redes adicionales. Consulte Opciones avanzadas de vSphere HA.

Redundancia de ruta de acceso de la red

La redundancia de ruta de acceso de la red entre nodos del clúster es importante para la confiabilidad de vSphere HA. Una sola red de administración termina siendo un único punto de error y puede dar como resultado conmutaciones por error aunque solo la red haya generado errores. Si tiene solo una red de administración, cualquier error entre el host y el clúster puede provocar una actividad de conmutación por error innecesaria (o falsa), en caso de que no se mantenga la conectividad del almacén de datos de latidos durante el error de redes. Entre los posibles errores se incluyen errores de NIC, de cables de red, de extracción de cables de red y de restablecimientos de conmutadores. Considere estas posibles fuentes de error entre hosts e intente minimizarlas, comúnmente mediante la entrega de redundancia de red.

La primera forma mediante la cual puede implementar redundancia de red es en el nivel de NIC con formación de equipos de NIC. El uso de un equipo de dos NIC conectadas para separar interruptores físicos separados mejora la confiabilidad de una red de administración. Debido a que los servidores conectados a través de dos NIC (y mediante conmutadores separados) tienen dos rutas de acceso independientes para enviar y recibir latidos, el clúster es más resistente. Para configurar un equipo de NIC para la red de administración, establezca las vNIC en la configuración de vSwitch para una configuración activa o en espera. Los parámetros de configuración recomendados para las vNICs son:

- Equilibrio de carga predeterminado = ruta basada en el identificador del puerto de origen
- Conmutación por recuperación = No

Después de que haya agregado una NIC a un host en su clúster de vSphere HA, debe volver a configurar vSphere HA en ese host.

En la mayoría de las implementaciones, la formación de equipos de NIC ofrece suficiente redundancia de latidos, pero como alternativa, puede crear una segunda conexión de red de administración conectada a un conmutador virtual separado. Las redes de administración redundante permite una detección confiable de errores y evita que se produzcan las condiciones de aislamiento o partición, ya que los latidos pueden enviarse a través de varias redes. La conexión de red de administración original se utiliza para fines de red y de administración. Cuando se crea la segunda conexión de red de administración, vSphere HA envía latidos a través de ambas conexiones de red de administración. Si hay error en una ruta de acceso, vSphere HA sigue enviando y recibiendo latidos a través de la otra ruta de acceso.

Nota Configure la menor cantidad posible de segmentos de hardware entre los servidores en un clúster. El objetivo es limitar puntos únicos de error. Además, las rutas con demasiados saltos pueden provocar retrasos de los paquetes de redes para latidos y aumentan los posibles puntos de error.

Usar configuraciones de red IPv6

Solo se puede asignar una dirección IPv6 a una interfaz de red determinada que usa su clúster de vSphere HA. La asignación de varias direcciones IP aumenta la cantidad de mensajes de latidos que envía el host principal del clúster sin un correspondiente beneficio.

Prácticas recomendadas para la interoperabilidad

Siga estas prácticas recomendadas para permitir una interoperabilidad entre vSphere HA y otras funciones.

Interoperabilidad de vSphere HA y Storage vMotion en un clúster mixto

No implemente vSphere HA en los clústeres donde están presentes los hosts ESXi 5.x y ESX/ESXi 4.1 o de versiones anteriores y donde se utiliza Storage vMotion ampliamente o Storage DRS está habilitado. vSphere HA puede responder a un error de host reiniciando una máquina virtual en un host con una versión de ESXi distinta a la versión en la que la máquina virtual se ejecutaba antes del error. Puede ocurrir un problema si, en el momento del error, la máquina virtual participaba en una acción de Storage vMotion en un host ESXi 5.x y vSphere HA reinicia la máquina virtual en un host de una versión anterior a ESXi 5.0. Si bien la máquina virtual puede encenderse, cualquier intento de operación de instantánea subsiguiente podría dañar el estado de vdisk y dejar la máquina virtual inutilizable.

Usar Auto Deploy con vSphere HA

Puede usar vSphere HA y Auto Deploy de forma conjunta para mejorar la disponibilidad de sus máquinas virtuales. Auto Deploy aprovisiona los hosts cuando se encienden y también se puede configurar para instalar el agente de vSphere HA en los hosts durante el proceso de arranque. Para conocer más detalles, consulte la documentación de Auto Deploy incluida en Instalar y configurar vSphere.

Actualizar hosts en un clúster mediante vSAN

Si va a actualizar los hosts ESXi en su clúster de vSphere HA a la versión 5.5 o una posterior y también tiene pensado usar vSAN, siga este proceso.

1 Actualice todos los hosts.

2 Deshabilite vSphere HA.

3 Habilite vSAN.

4 Vuelva a habilitar vSphere HA.

Prácticas recomendadas para supervisión de clústeres

Siga estas prácticas recomendadas para supervisar el estado y validez de su clúster de vSphere HA.

Configurar alarmas para supervisar cambios del clúster

Cuando vSphere HA o Fault Tolerance toman medidas para mantener la disponibilidad, por ejemplo, una conmutación por error de máquina virtual, puede recibir notificaciones de dichos cambios. Configure alarmas en vCenter Server para que se activen cuando se produzcan estas acciones y haga que se envíen las alertas (como correos electrónicos) a un conjunto específico de administradores.

Hay varias alarmas predeterminadas de vSphere HA disponibles.

- Recursos insuficientes para conmutación por error (una alarma de clúster)
- No se puede encontrar un elemento principal (una alarma de clúster)
- Conmutación por error en curso (una alarma de clúster)
- Estado de HA del host (una alarma de host)
- Error de supervisión de máquina virtual (una alarma de máquina virtual)
- Acción de supervisión de máquina virtual (una alarma de máquina virtual)
- Error de conmutación por error (una alarma de máquina virtual)

Nota Las alarmas predeterminadas incluyen el nombre de la característica, vSphere HA.

Proporcionar Fault Tolerance para máquinas virtuales

3

Puede utilizar vSphere Fault Tolerance para las máquinas virtuales a fin de garantizar la continuidad de mayores niveles de disponibilidad y protección de datos.

Fault Tolerance está integrado en la plataforma de host ESXi y proporciona disponibilidad mediante la ejecución de máquinas virtuales idénticas en hosts distintos.

Para lograr resultados óptimos con Fault Tolerance, es necesario familiarizarse con su modo de funcionamiento, la forma de habilitarlo para el clúster y las máquinas virtuales, y las prácticas recomendadas para su uso.

Este capítulo incluye los siguientes temas:

Funcionamiento de Fault Tolerance

Puede utilizar vSphere Fault Tolerance (FT) para la mayoría de las máquinas virtuales de misión crítica. FT ofrece disponibilidad continua para máquinas virtuales de este tipo mediante la creación y el mantenimiento de máquinas virtuales idénticas y con disponibilidad continua para reemplazarlas en caso de una situación de conmutación por error.

La máquina virtual protegida se conoce como la máquina virtual principal. La máquina virtual duplicada (la secundaria) se crea y ejecuta en otro host. La ejecución de la máquina virtual secundaria es idéntica a la de la máquina virtual principal y puede asumir su control en cualquier punto sin interrupción, con lo que proporciona protección con Fault Tolerance.

Las máquinas virtuales principales y secundarias supervisan de forma continua sus estados mutuos a fin de asegurar que se mantenga Fault Tolerance. Si hay error del host que ejecuta la máquina virtual principal, se produce una conmutación por error transparente, en cuyo caso la máquina virtual secundaria se activa inmediatamente para reemplazar la máquina virtual principal. Se inicia una nueva máquina virtual secundaria y la redundancia de Fault Tolerance se restablece automáticamente. Si se produce un error en el host que ejecuta la máquina virtual secundaria, también se reemplaza de inmediato. En cualquier caso, los usuarios no experimentan interrupción en el servicio ni hay pérdida de datos.

Una máquina virtual con Fault Tolerance y su copia secundaria no deben ejecutarse en el mismo host. Esta restricción asegura que, si hay un error del host, ello no redunde en una pérdida de ambas máquinas virtuales.

Nota También puede utilizar las reglas de afinidad Máquina virtual-Host para indicar en qué hosts pueden funcionar las máquinas virtuales designadas. Si utiliza estas reglas, tenga en cuenta que para cualquier máquina virtual principal que se vea afectada por dicha regla, su máquina virtual secundaria asociada también se verá afectada por esa regla. Para obtener más información acerca de reglas de afinidad, consulte la documentación de *Administración de recursos de vSphere*.

Fault Tolerance evita situaciones de "cerebro dividido", lo que puede derivar en dos copias activas de una máquina virtual después de una recuperación de un error. El bloqueo de archivos atómico en almacenamiento compartido se utiliza para coordinar conmutación por error de manera que solo un lado siga en ejecución como la máquina virtual principal y reaparezca automáticamente una nueva máquina virtual secundaria.

vSphere Fault Tolerance puede aceptar máquinas virtuales con multiprocesador simétrico (SMP) con hasta cuatro vCPU. Versiones anteriores de vSphere utilizaban una tecnología diferente para Fault Tolerance (que se conoce como FT heredada), con distintos requisitos y características (incluida una limitación de vCPU únicas para máquinas virtuales de FT heredadas). Si se requiere compatibilidad con estos requisitos anteriores, puede utilizar FT heredada. Sin embargo, esto implica la configuración de una opción avanzada para cada máquina virtual. Consulte Fault Tolerance heredado para obtener más información.

Casos de uso de Fault Tolerance

Hay varias situaciones típicas que pueden aprovechar el uso de vSphere Fault Tolerance.

Fault Tolerance proporciona un mayor nivel de continuidad empresarial que vSphere HA. Cuando se solicita a una máquina virtual secundaria que reemplace a su máquina virtual principal, la máquina virtual secundaria asume de inmediato el control de la función de la máquina virtual principal y se mantiene la totalidad del estado de la máquina virtual. Las aplicaciones ya están en ejecución y no es necesario volver a introducir o cargar los datos almacenados en la memoria. La conmutación por error proporcionada por vSphere HA reinicia las máquinas virtuales afectadas por un error.

Este mayor nivel de continuidad, así como la protección adicional de la información del estado y de los datos, informa sobre los escenarios en los que es conveniente implementar Fault Tolerance.

- Las aplicaciones que siempre deben estar disponibles, especialmente aquellas que tienen conexiones de clientes de larga duración que los usuarios quieren mantener durante un error de hardware.
- Las aplicaciones personalizadas que no tienen otra forma de agrupar en clústeres.
- Los casos donde podría proporcionarse alta disponibilidad mediante soluciones personalizadas de creación de clústeres, que son demasiado complicadas para configurar y mantener.

Otro caso de uso clave para proteger una máquina virtual con Fault Tolerance puede describirse como On-Demand Fault Tolerance. En este caso, una máquina virtual se protege adecuadamente con vSphere HA durante el funcionamiento normal. Durante ciertos períodos críticos, sería recomendable mejorar la protección de la máquina virtual. Por ejemplo, podría estar ejecutando un informe de fin de trimestre que, si se interrumpe, retrasaría la disponibilidad de información crítica. Con vSphere Fault Tolerance, puede proteger esta máquina virtual antes de ejecutar ese informe y después apagar o suspender Fault Tolerance una vez que se haya generado el informe. Puede usar On-Demand Fault Tolerance para proteger la máquina virtual durante un período de tiempo crítico y volver los recursos a la normalidad durante la operación no crítica.

Requisitos, límites y concesión de licencias de Fault Tolerance

Antes de usar vSphere Fault Tolerance (FT), considere los requisitos, los límites y la concesión de licencias de alto nivel que se aplican a esta característica.

Requisitos

Los siguientes requisitos de CPU y redes se aplican a FT.

Las CPU que se utilizan en máquinas host para máquina virtual con Fault Tolerance deben ser compatibles con vSphere vMotion o estar mejoradas con Enhanced vMotion Compatibility. Igualmente, se requieren CPU que admitan virtualización de MMU de hardware (Intel EPT o RVI AMD). Se admiten las siguientes CPU.

- Intel Sandy Bridge o posterior. Avoton no es compatible.
- AMD Bulldozer o posterior.

Use una red de registro de 10 Gbit para FT y verifique que la red tenga baja latencia. Se recomienda contar con una red de FT dedicada.

Límites

En un clúster configurado para que use Fault Tolerance, se aplican dos límites de forma independiente.

das.maxftvmsperhost

La cantidad máxima de máquinas virtuales con Fault Tolerance que se permiten en un host en el clúster. Tanto las máquinas virtuales principales como las secundarias se contabilizan para este límite. El valor predeterminado es 4.

das.maxftvcpusperhost

La cantidad máxima de CPU que se agregan por todas las máquinas virtuales con Fault Tolerance en un host. Para este límite se contabilizan tanto las vCPU de máquinas virtuales principales como las de máquinas virtuales secundarias. El valor predeterminado es 8.

Licencias

La cantidad de vCPU que admite una sola máquina virtual con Fault Tolerance está limitada por el nivel de licencias que haya adquirido para vSphere. Fault Tolerance se admite de las siguientes maneras:

- vSphere Standard y Enterprise. Permite hasta 2 vCPU.
- vSphere Enterprise Plus. Permite hasta 4 vCPU.

Nota FT y FT heredado no se admiten en vSphere Essentials y vSphere Essentials Plus.

Interoperabilidad de Fault Tolerance

vSphere Fault Tolerance se enfrenta a algunas limitaciones con respecto a las características de vSphere, los dispositivos y otras características con las que puede interoperar.

Antes de configurar vSphere Fault Tolerance, debe conocer las funciones y los productos con los que Fault Tolerance no puede interoperar.

Características de vSphere no compatibles con Fault Tolerance

Cuando configure el clúster, debe tener en cuenta que no todas las características de vSphere pueden interoperar con Fault Tolerance.

Las siguientes características de vSphere no son compatibles con las máquinas virtuales con Fault Tolerance.

- Instantáneas. Las instantáneas deben quitarse o confirmarse antes de que sea posible habilitar Fault Tolerance en una máquina virtual. Además, no es posible crear instantáneas de máquinas virtuales en las que esté habilitado Fault Tolerance.

  Nota Las instantáneas solo de disco creadas para las copias de seguridad de vStorage APIs - Data Protection (VADP) son compatibles con Fault Tolerance. Sin embargo, FT heredado no es compatible con VADP.

- Storage vMotion. No puede invocar Storage vMotion para máquinas virtuales con Fault Tolerance activado. Para migrar el almacenamiento, debe desactivar temporalmente Fault Tolerance y realizar la acción de vMotion para almacenamiento. Cuando esto haya concluido, puede volver a activar Fault Tolerance.
- Clones vinculados. No puede usar Fault Tolerance en una máquina virtual que sea un clon vinculado, ni tampoco puede crear un clon vinculado a partir de una máquina virtual con FT habilitado.
- VM Component Protection (VMCP) (Protección de componentes de la máquina virtual [VMCP]). Si su clúster tiene VMCP habilitado, se crean anulaciones para las máquinas virtuales con Fault Tolerance que desactivan esta característica.
- Almacenes de datos de Virtual Volumes.
- Administración de directivas basadas en almacenamiento.
- Filtros de E/S.

Características y dispositivos incompatibles con Fault Tolerance

No todos los dispositivos, características o productos de terceros pueden interoperar con Fault Tolerance.

Para que una máquina virtual sea compatible con Fault Tolerance, dicha máquina no debe usar las siguientes características o dispositivos.

Tabla 3-1. Características y dispositivos incompatibles con Fault Tolerance y acciones correctivas

Característica o dispositivo incompatible	Acción correctiva
Asignación de disco sin procesar (RDM) física.	Con FT heredado, puede volver a configurar máquinas virtuales con dispositivos virtuales a los que se les hizo una copia de seguridad con RDM física para usar RMD virtuales en su lugar.
Dispositivos virtuales en CD-ROM y disquete cuya copia de seguridad se hizo mediante un dispositivo físico o remoto.	Quite el dispositivo virtual en CD-ROM o disquete y vuelva a configurar la copia de seguridad con un ISO instalado en el almacenamiento compartido.
Dispositivos USB y de sonido.	Quite estos dispositivos de la máquina virtual
Virtualización de identificador de puerto N (NPIV).	Deshabilite la configuración de NPIV de la máquina virtual.

Tabla 3-1. Características y dispositivos incompatibles con Fault Tolerance y acciones correctivas (continuación)

Característica o dispositivo incompatible	Acción correctiva
Acceso directo de la NIC.	Esta característica no es compatible con Fault Tolerance por lo que debe desactivarse.
Dispositivos de conexión directa.	La característica de conexión en caliente se deshabilita de forma automática para máquinas virtuales con Fault Tolerance. Para conectar dispositivos en caliente (ya sea mediante adición o extracción), debe desactivar temporalmente Fault Tolerance, realizar la conexión directa y luego habilitar Fault Tolerance. **Nota** Cuando se utiliza Fault Tolerance, el cambio de la configuración de una tarjeta de red virtual mientras una máquina virtual está en ejecución corresponde a una operación de conexión directa, ya que en necesario "desconectar" la tarjeta de red y luego volver a "conectarla". Por ejemplo, con una tarjeta de red virtual para una máquina virtual en ejecución, si cambia la red a la que está conectada la NIC virtual, primero debe desactivarse FT.
Puertos serie o paralelos	Quite estos dispositivos de la máquina virtual
Dispositivos de vídeo que tienen 3D habilitado.	Fault Tolerance no es compatible con dispositivos de vídeo que tienen 3D habilitado.
Firmware EFI virtual	Asegúrese de que la máquina virtual esté configurada para que utilice firmware del BIOS antes de instalar el sistema operativo invitado.
Interfaz de comunicación de máquina virtual (VMCI)	No compatible con Fault Tolerance.
VMDK de más de 2 TB	Fault Tolerance no es compatible con un VMDK de más de 2 TB.

Usar Fault Tolerance con DRS

Puede usar vSphere Fault Tolerance con vSphere Distributed Resource Scheduler (DRS) solo cuando está habilitada la función Enhanced vMotion Compatibility (EVC). Este proceso permite que las máquinas virtuales con Fault Tolerance se beneficien de una mejor colocación inicial.

Cuando un clúster tiene EVC habilitado, DRS hace las recomendaciones de colocación inicial para las máquinas virtuales con Fault Tolerance y permite asignar un nivel de automatización de DRS a las máquinas virtuales principales (la máquina virtual secundaria siempre supone la misma configuración que su máquina virtual principal asociada).

Cuando vSphere Fault Tolerance se utiliza para máquinas virtuales en un clúster que tiene EVC deshabilitado, se otorgan niveles de automatización de DRS de "disabled" (deshabilitado) a las máquinas virtuales con Fault Tolerance. En dicho clúster, cada máquina virtual principal se enciende solo en su host registrado y su máquina virtual secundaria se coloca automáticamente.

Si utiliza reglas de afinidad con un par de máquinas virtuales con Fault Tolerance, se aplica una regla de afinidad Máquina virtual-Máquina virtual solo a la máquina virtual principal, mientras que una regla de afinidad Máquina virtual-Host se aplica tanto a la máquina virtual principal como a su máquina virtual secundaria. Si se establece una regla de afinidad Máquina virtual-Máquina virtual para una máquina virtual principal, DRS intenta corregir cualquier infracción que se produzca después de una conmutación por error (es decir, después de que la máquina virtual principal se mueve a un nuevo host).

Site Recovery Manager

Site Recovery Manager 6.5.1 no admite la protección de máquinas virtuales configuradas con una instancia de vSphere Fault Tolerance (FT) con varias CPU. Site Recovery Manager 6.5.1 admite la protección de máquinas virtuales con una instancia de vSphere FT con monoprocesador, pero desactiva dicha instancia en las máquinas virtuales del sitio de recuperación tras una recuperación.

- Si utiliza una instancia de vSphere FT con varias CPU en máquinas virtuales, Site Recovery Manager no la desactiva en las máquinas virtuales recuperadas y se produce un error al encender dichas máquinas virtuales. Debe desactivar vSphere FT manualmente en las máquinas virtuales recuperadas quitando las propiedades de FT y volviendo a ejecutar el plan de recuperación.
- Si utiliza una instancia de vSphere FT con monoprocesador en las máquinas virtuales, deberá configurar las máquinas virtuales en el sitio protegido de modo que Site Recovery Manager pueda desactivar vSphere FT tras una recuperación. Para obtener información sobre la configuración de las máquinas virtuales para una instancia de vSphere FT con monoprocesador en el sitio protegido, consulte http://kb.vmware.com/kb/2109813.

Para obtener más información, consulte *VMware Site Recovery Manager*.

Preparar el clúster y los hosts para Fault Tolerance

Para habilitar vSphere Fault Tolerance en el clúster, debe cumplir con los requisitos previos de la característica y seguir ciertos pasos de configuración en los hosts. Una vez completados esos pasos y creado el clúster, también puede comprobar que la configuración cumpla con los requisitos para habilitar Fault Tolerance.

Las tareas que se deben completar antes de intentar configurar Fault Tolerance en el clúster son las siguientes:

- Asegúrese de que el clúster, los hosts y las máquinas virtuales cumplan con los requisitos descritos en la lista de comprobación de Fault Tolerance.
- Configure las redes para cada host.
- Cree el clúster de vSphere HA, agregue hosts y compruebe el cumplimiento.

Una vez preparados el clúster y los hosts para Fault Tolerance, ya estará listo para activar Fault Tolerance en las máquinas virtuales. Consulte Activar Fault Tolerance.

Lista de comprobación de Fault Tolerance

La siguiente lista de comprobación contiene requisitos de clúster, host y máquina virtual que se deben tener en cuenta antes de utilizar vSphere Fault Tolerance.

Revise la lista antes de configurar Fault Tolerance.

Nota La conmutación por error de las máquinas virtuales con tolerancia a errores es independiente de vCenter Server, pero se debe utilizar vCenter Server para configurar los clústeres de Fault Tolerance.

Requisitos de clúster para Fault Tolerance

Se deben cumplir los siguientes requisitos de clúster antes de utilizar Fault Tolerance.

- El registro de Fault Tolerance y las redes de VMotion deben estar configurados. Consulte Configurar redes para equipos host.
- Se debe haber creado y habilitado el clúster de vSphere HA. Consulte Crear un clúster de vSphere HA. vSphere HA debe estar habilitado para poder encender las máquinas virtuales con tolerancia a errores o para agregar un host a un clúster que ya admite máquinas virtuales con tolerancia a errores.

Requisitos de host para Fault Tolerance

Se deben cumplir los siguientes requisitos de host antes de utilizar Fault Tolerance.

- Los hosts deben utilizar procesadores compatibles.
- Los hosts deben tener licencia para Fault Tolerance.
- Los hosts deben estar certificados para Fault Tolerance. Consulte http://www.vmware.com/resources/compatibility/search.php y seleccione **Buscar por conjuntos compatibles con tolerancia a errores** para determinar si los hosts están certificados.
- La configuración para cada host debe tener habilitada la virtualización de hardware (HV) en el BIOS.

Nota VMware recomienda que la configuración de administración de energía del BIOS de los hosts que se utilicen para admitir máquinas virtuales de FT esté definida en Rendimiento máximo o Rendimiento administrado por sistema operativo.

Para confirmar la compatibilidad de los hosts en el clúster a fin de admitir Fault Tolerance, se pueden ejecutar comprobaciones de cumplimiento de perfiles como se describe en Crear un clúster y comprobar el cumplimiento.

Requisitos de la máquina virtual para Fault Tolerance

Se deben cumplir los siguientes requisitos de máquina virtual antes de utilizar Fault Tolerance.

- No debe haber ningún dispositivo no compatible conectado a la máquina virtual. Consulte Interoperabilidad de Fault Tolerance.

- Las características no compatibles no se deben ejecutar en máquinas virtuales con tolerancia a errores. Consulte Interoperabilidad de Fault Tolerance.
- Los archivos de la máquina virtual (excepto los archivos VMDK) se deben guardar en el almacenamiento compartido. Las soluciones aceptables de almacenamiento compartido incluyen canal de fibra, iSCSI (hardware y software), NFS y NAS.

Otras recomendaciones de configuración

Se deben cumplir las siguientes instrucciones al configurar Fault Tolerance.

- Si se utiliza NFS para acceder al almacenamiento compartido, utilice hardware de NAS dedicado con al menos una NIC de 1 Gbit para obtener el rendimiento de red requerido para que Fault Tolerance funcione correctamente.
- La reserva de memoria de una máquina virtual con tolerancia a errores se establece de acuerdo con el tamaño de memoria de la máquina virtual cuando Fault Tolerance está activado. Compruebe que un grupo de recursos que contenga máquinas virtuales con tolerancia a errores tenga recursos de memoria cuyo tamaño de memoria sea mayor que el de las máquinas virtuales. Sin este exceso en el grupo de recursos, es posible que no haya memoria disponible para utilizar como memoria de sobrecarga.
- Utilice un máximo de 16 discos virtuales por máquina virtual con tolerancia a errores.
- Para garantizar la redundancia y una protección óptima de Fault Tolerance, se deben tener tres hosts en el clúster como mínimo. Durante una situación de conmutación por error, esto proporciona un host que puede alojar la nueva máquina virtual secundaria que se crea.

Configurar redes para equipos host

En cada host que desee agregar a un clúster de vSphere HA, deberá configurar dos conmutadores de redes diferentes (vMotion y registro de FT), de manera que el host pueda admitir vSphere Fault Tolerance.

Para configurar Fault Tolerance para un host, debe realizar este procedimiento para cada opción de grupo de puertos (vMotion y registro de FT) a fin de asegurar que haya suficiente ancho de banda disponible para el registro de Fault Tolerance. Seleccione una opción, finalice este procedimiento y repítalo una segunda vez seleccionando la otra opción de grupo de puertos.

Requisitos previos

Se requieren tarjetas de interfaz de red (NIC) de varios gigabits. Para cada host compatible con Fault Tolerance, se recomienda un mínimo de dos NIC físicas. Por ejemplo, se necesita una dedicada al registro de Fault Tolerance y una dedicada a vMotion. Utilice tres NIC o más para garantizar la disponibilidad.

Nota Las NIC de vMotion y de registro de FT deben estar en diferentes subredes. Si va a utilizar FT heredada, IPv6 no es compatible en la NIC de registro de FT.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.
2 Haga clic en la pestaña **Configurar** y en **Redes**.
3 Seleccione **Adaptador de red de VMkernel**.
4 Haga clic en el icono **Agregar redes de host**.
5 Proporcione información adecuada para el tipo de conexión.
6 Haga clic en **Finalizar**.

Resultados

Después de crear un conmutador virtual de registro de Fault Tolerance y vMotion, puede crear otros conmutadores virtuales según sea necesario. Agregue el host al clúster y finalice cualquier paso necesario para habilitar Fault Tolerance.

Pasos siguientes

Nota Si configura redes para admitir FT, pero posteriormente suspende el puerto de registro de Fault Tolerance, los pares de máquinas virtuales de Fault Tolerance, que se enciendan permanecerán encendidos. Si se produce una situación de conmutación por error, cuando la máquina virtual principal se reemplaza con su máquina virtual secundaria, no se inicia una nueva máquina virtual secundaria, con lo que la nueva máquina virtual principal se ejecuta en un estado Sin protección.

Crear un clúster y comprobar el cumplimiento

vSphere Fault Tolerance se utiliza en el contexto de un clúster de vSphere HA. Después de configurar las redes en cada host, cree el clúster de vSphere HA y agréguele hosts. Puede comprobar si el clúster está configurado correctamente y si cumple con los requisitos para la habilitación de Fault Tolerance.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster.
2 Haga clic en la pestaña **Monitor** (Supervisar) y luego en **Profile Compliance** (Cumplimiento del perfil).
3 Haga clic en **Check Compliance Now** (Comprobar cumplimiento ahora) para ejecutar las pruebas de cumplimiento.

Resultados

Aparecen los resultados de la prueba de cumplimiento y se muestra el cumplimiento o el incumplimiento de cada host.

Usar Fault Tolerance

Después de que haya realizado todos los pasos necesarios para habilitar vSphere Fault Tolerance para el clúster, puede utilizar la característica habilitándola para máquinas virtuales individuales.

Antes de que se pueda activar Fault Tolerance, se realizan comprobaciones de validación en una máquina virtual.

Después de pasar las comprobaciones y de activar vSphere Fault Tolerance para una máquina virtual, se agregan nuevas opciones a la sección a la sección de Fault Tolerance de su menú contextual. Entre estas se incluyen la desactivación o deshabilitación de Fault Tolerance, la migración de la máquina virtual secundaria, las pruebas de conmutación por error y las pruebas de reinicio de la máquina virtual secundaria.

Realizar comprobaciones de validación para activación de Fault Tolerance

Si la opción para activar Fault Tolerance se encuentra disponible, esta tarea aún debe validarse y puede generar errores si no se cumplen ciertos requisitos.

Antes de poder activar Fault Tolerance, se realizan varias comprobaciones de validación en una máquina virtual.

- Debe estar activada la comprobación de certificado SSL en la configuración de vCenter Server.
- El host debe estar en un clúster de vSphere HA o un clúster mixto de vSphere HA y DRS.
- El host debe tener ESXi 6.x o una versión superior instalada (ESX/ESXi 4.x o versión superior para FT heredado).
- La máquina virtual no debe tener instantáneas.
- La máquina virtual no debe ser una plantilla.
- La máquina virtual no debe tener vSphere HA deshabilitado.
- La máquina virtual no debe tener un dispositivo de vídeo con 3D habilitado.

Comprobar si existen máquinas virtuales encendidas

Se realizan varias comprobaciones de validación adicionales para máquinas virtuales encendidas (o aquellas que están en proceso de encendido).

- El BIOS de los hosts donde se encuentran las máquinas virtuales con Fault Tolerance deben tener habilitado Hardware Virtualization (HV) (Virtualización de hardware).
- El host que admite la máquina virtual principal debe tener un procesador que sea compatible con Fault Tolerance.
- Su hardware debe contar con certificación de compatibilidad con Fault Tolerance. Para confirmar que la tiene, use la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php y seleccione **Search by Fault Tolerant Compatible Sets** (Buscar por conjuntos compatibles con Fault Tolerance).

- La configuración de la máquina virtual debe ser válida para usar con Fault Tolerance (por ejemplo, no debe contener ningún dispositivo no compatible).

Colocación de máquina virtual secundaria

Cuando su trabajo de activación de Fault Tolerance para una máquina virtual pasa las comprobaciones de validación, se crea la máquina virtual secundaria. La colocación y estado inmediato de la máquina virtual secundaria depende de si se encendió o apagó la máquina virtual principal cuando encendió Fault Tolerance.

Si la máquina virtual principal está encendida:

- Si pasa el control de admisión, se copia el estado completo de la máquina virtual principal y la máquina virtual secundaria se crea, se coloca en un host compatible separado y se enciende.
- El estado de Fault Tolerance que aparece para la máquina virtual es **Protected** (Protegida).

Si la máquina virtual principal está apagada:

- Se crea de inmediato la máquina virtual secundaria y se registra en un host en el clúster (podría volver a registrarse en un host más apropiado cuando se encienda).
- La máquina virtual secundaria no se enciende hasta después de que lo hace la máquina virtual principal.
- El estado de Fault Tolerance que aparece para la máquina virtual es **Not Protected, VM not Running** (No protegido, máquina virtual no está funcionando).
- Cuando intenta encender la máquina virtual principal después de que se ha encendido Fault Tolerance, se realizan las comprobaciones de validación adicionales que se indicaron más arriba.

  Después de pasar todas estas comprobaciones, las máquinas virtuales principales y secundarias se encienden y se colocan en hosts compatibles separados. El estado de Fault Tolerance de la máquina virtual se etiqueta como **Protected** (Protegida).

Activar Fault Tolerance

Puede activar vSphere Fault Tolerance mediante vSphere Web Client.

Cuando Fault Tolerance está activado, vCenter Server restablece el límite de memoria de la máquina virtual y configura la reserva de memoria en el tamaño de memoria de la máquina virtual. Aunque Fault Tolerance permanezca activado, no es posible cambiar la reserva, el tamaño y el límite de memoria, la cantidad de vCPU o los recursos compartidos. Tampoco puede agregar ni quitar discos de la máquina virtual. Cuando Fault Tolerance está apagado, cualquier parámetro que se haya cambiado no se revierte a los valores originales.

Conecte vSphere Web Client a vCenter Server utilizando una cuenta con permisos de administrador de clúster.

Requisitos previos

La opción para activar Fault Tolerance no se encuentra disponible (atenuada) en caso de que se aplique cualquiera de estas condiciones:

- La máquina virtual se encuentra en un host que no tiene una licencia para la característica.
- La máquina virtual se encuentra en un host que está en modo de mantenimiento o de espera.
- La máquina virtual está desconectada o huérfana (no se puede acceder a su archivo .vmx).
- El usuario no tiene permisos para activar la característica.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual para la cual desea activar Fault Tolerance.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Turn On Fault Tolerance (Activar Fault Tolerance)**.

3 Haga clic en **Yes** (Sí).

4 Seleccione un almacén de datos para colocar los archivos de configuración de la máquina virtual secundaria. A continuación, haga clic en **Next** (Siguiente).

5 Seleccione un host en el que colocar la máquina virtual secundaria. A continuación, haga clic en **Next** (Siguiente).

6 Revise las selecciones y, a continuación, haga clic en **Finish** (Finalizar).

Resultados

La máquina virtual especificada está designada como máquina virtual principal, y una máquina virtual secundaria se establece en otro host. La máquina virtual principal ahora tiene tolerancia a errores.

Desactivar Fault Tolerance

Si se desactiva vSphere Fault Tolerance, se eliminan la máquina virtual secundaria, su configuración y todo el historial.

Utilice la opción **Turn Off Fault Tolerance** (Desactivar Fault Tolerance) si no tiene pensado volver a habilitar la característica. De lo contrario, utilice la opción **Suspend Fault Tolerance** (Suspender Fault Tolerance).

Nota Si la máquina virtual secundaria reside en un host que está en modo de mantenimiento, desconectado o que no responde, no se puede utilizar la opción **Turn Off Fault Tolerance** (Desactivar Fault Tolerance). En este caso, debe suspender y reanudar Fault Tolerance.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual para la cual desea desactivar Fault Tolerance.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Turn Off Fault Tolerance (Desactivar Fault Tolerance)**.

3 Haga clic en **Yes** (Sí).

Resultados

Fault Tolerance se desactiva en la máquina virtual seleccionada. Se eliminarán el historial y la máquina virtual secundaria de la máquina virtual seleccionada.

Suspender Fault Tolerance

La suspensión de vSphere Fault Tolerance para una máquina virtual suspende su protección de Fault Tolerance, pero mantiene la máquina virtual secundaria y todo el historial. Use esta opción para reanudar la protección de Fault Tolerance en el futuro.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual para la cual desea suspender Fault Tolerance.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Suspend Fault Tolerance (Suspender Fault Tolerance)**.

3 Haga clic en **Yes** (Sí).

Resultados

Fault Tolerance se suspende para la máquina virtual seleccionada. Todo el historial y la máquina virtual secundaria de la máquina virtual seleccionada se mantienen y se usarán en caso de que se reanude la característica.

Pasos siguientes

Después de suspender Fault Tolerance, para reanudar la característica, seleccione **Resume Fault Tolerance** (Reanudar Fault Tolerance).

Migrar máquina secundaria

Una vez que vSphere Fault Tolerance se encienda para una máquina virtual principal, podrá migrar su máquina virtual secundaria asociada.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual principal para la cual desea migrar su máquina virtual secundaria.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Migrate Secondary (Migrar máquina secundaria)**.

3 Siga las opciones en el cuadro de diálogo Migrate (Migrar) y confirme los cambios que ha realizado.

4 Haga clic en **Finish** (Finalizar) para aplicar los cambios.

Resultados

La máquina virtual secundaria asociada a la máquina virtual con tolerancia a errores se migra al host especificado.

Probar conmutación por error

Es posible inducir una situación de conmutación por error de una máquina virtual principal seleccionada a fin de probar la protección de Fault Tolerance.

Esta opción no se encuentra disponible (está atenuada) si la máquina virtual está apagada.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual principal en la cual desea probar la conmutación por error.
2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Test Failover (Probar conmutación por error)**.
3 Vea detalles sobre la conmutación por error en la consola de la tarea.

Resultados

Esta tarea induce un error en la máquina virtual principal para garantizar que la máquina virtual secundaria la reemplace. También se inicia una nueva máquina virtual secundaria cuando se vuelve a colocar la máquina virtual principal en estado protegido.

Probar reinicio de la máquina secundaria

Puede inducir el error de una máquina virtual secundaria para probar la protección Fault Tolerance provista para una máquina virtual principal seleccionada.

Esta opción no se encuentra disponible (está atenuada) si la máquina virtual está apagada.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual principal en la cual desea realizar la prueba.
2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Test Restart Secondary (Probar reinicio de máquina secundaria)**.
3 Vea detalles sobre la prueba en la consola de la tarea.

Resultados

Esta tarea da como resultado la terminación de la máquina virtual secundaria que brinda protección Fault Tolerance a la máquina virtual principal seleccionada. Se inicia una nueva máquina virtual secundaria, que vuelve a poner la máquina virtual principal en un estado Protected (Protegida).

Actualizar los hosts utilizados para Fault Tolerance

Use el siguiente procedimiento para actualizar los hosts que se usan para Fault Tolerance.

Requisitos previos

Compruebe que dispone de privilegios de administrador del clúster.

Compruebe que tiene conjuntos de cuatro o más hosts ESXi que alojen máquinas virtuales con Fault Tolerance que estén encendidas. Si las máquinas virtuales están apagadas, las máquinas virtuales principales y secundarias se pueden reubicar en hosts con diferentes compilaciones.

Nota Este procedimiento de actualización es para un clúster con un mínimo de cuatro nodos. Se pueden seguir las mismas instrucciones para un clúster de menor tamaño, aunque el intervalo sin protección será ligeramente más prolongado.

Procedimiento

1. Utilice vMotion para migrar las máquinas virtuales con Fault Tolerance desde dos hosts.
2. Actualice los dos hosts evacuados a la misma compilación de ESXi.
3. Suspenda Fault Tolerance en la máquina virtual principal.
4. Utilice vMotion para mover la máquina virtual principal para la cual Fault Tolerance se haya suspendido a uno de los hosts actualizados.
5. Reanude Fault Tolerance en la máquina virtual principal que se movió.
6. Repita del Paso 1 al Paso 5 para tantos pares de máquinas virtuales con Fault Tolerance como se puedan aceptar en los hosts actualizados.
7. Utilice vMotion para redistribuir las máquinas virtuales con Fault Tolerance.

Resultados

Todos los hosts ESXi de un clúster estarán actualizados.

Prácticas recomendadas de Fault Tolerance

Para garantizar resultados óptimos con Fault Tolerance, se deben seguir ciertas prácticas recomendadas.

Las siguientes recomendaciones para la configuración de hosts y redes pueden ayudar a mejorar la estabilidad y el rendimiento del clúster.

Configuración de hosts

Los hosts que ejecutan las máquinas virtuales principales y secundarias deben operar aproximadamente a la misma frecuencia de procesador. Las características de administración de energía de la plataforma que no se ajusten según la carga de trabajo (por ejemplo, topes de energía y modos de baja frecuencia aplicados para ahorrar energía) pueden provocar una

gran variación en la frecuencia del procesador. Si las máquinas virtuales secundarias se reinician de manera regular, deshabilite todos los modos de administración de energía en los hosts que ejecutan máquinas virtuales con tolerancia a errores o compruebe que todos los hosts se ejecuten en los mismos modos de administración de energía.

Configurar redes del host

Las siguientes instrucciones permiten configurar las redes del host para que admitan Fault Tolerance con diferentes combinaciones de tipos de tráfico (por ejemplo, NFS) y números de NIC físicas.

- Distribuya cada equipo de NIC en dos conmutadores físicos para garantizar la continuidad del dominio L2 de cada VLAN entre los dos conmutadores físicos.
- Utilice directivas de formación de equipos determinísticas para garantizar que tipos de tráfico específicos tengan una afinidad con una NIC determinada (activa/en espera) o un grupo de NIC (por ejemplo, identificador de puerto virtual de origen).
- En casos donde se utilicen directivas activas/en espera, vincule los tipos de tráfico para minimizar el impacto en una situación de conmutación por error donde los dos tipos de tráfico comparten una vmnic.
- En casos donde se utilicen directivas activas/en espera, configure todos los adaptadores activos para un tipo de tráfico específico (por ejemplo, registro de FT) en el mismo conmutador físico. Esto minimiza la cantidad de saltos de red y disminuye la posibilidad de que se produzca un exceso de suscripciones del conmutador en vínculos del conmutador.

Nota El tráfico de registro de FT entre la máquina virtual principal y la secundaria está descifrado y contiene datos de la red invitada y de la E/S de almacenamiento, como también contenido de memoria del sistema operativo invitado. Este tráfico puede incluir datos sensibles como contraseñas en texto sin formato. Para evitar que estos datos se divulguen, asegúrese de que la red esté protegida, especialmente contra ataques de intermediarios ("Man in the middle"). Por ejemplo, puede utilizar una red privada para el tráfico de registro de FT.

Clústeres homogéneos

vSphere Fault Tolerance puede funcionar en clústeres con hosts no uniformes, pero funciona mejor en clústeres con nodos compatibles. Al construir su clúster, todos los hosts deben tener la siguiente configuración:

- Acceso común a los almacenes de datos utilizados por las máquinas virtuales.
- La misma configuración de red de la máquina virtual.
- La misma configuración del BIOS (administración de energía e hiperproceso) para todos los hosts.

Ejecute **Comprobar cumplimiento** para identificar incompatibilidades y corregirlas.

Rendimiento

Para aumentar el ancho de banda disponible para el tráfico de registro entre máquinas virtuales principales y secundarias, se utiliza una NIC de 10 Gbit y se habilita la utilización de tramas gigantes.

Puede seleccionar varias NIC para la red de registro de FT. Al seleccionar varias NIC, puede aprovechar el ancho de banda de todas las NIC incluso si estas no se utilizan exclusivamente para ejecutar FT.

ISO en almacenamiento compartido para acceso continuo

Almacene las imágenes ISO a las que acceden las máquinas virtuales con la función Fault Tolerance habilitada en un almacenamiento compartido al que puedan acceder ambas instancias de la máquina virtual con tolerancia a errores. Si se utiliza esta configuración, el CD-ROM de la máquina virtual sigue funcionando con normalidad, incluso cuando ocurre una conmutación por error.

Para máquinas virtuales con la función Fault Tolerance habilitada, se pueden utilizar imágenes ISO que sean accesibles solo para la máquina virtual principal. En este caso, la máquina virtual principal puede acceder a la imagen ISO; pero si se produce una conmutación por error, el CD-ROM informa de errores como si no hubiera soportes físicos. Esta situación puede ser aceptable si el CD-ROM se utiliza para una operación temporal y no crítica (por ejemplo, una revisión).

Evitar particiones de red

Una partición de red se produce cuando un clúster de vSphere HA tiene un error en la red de administración que aísla algunos de los hosts de vCenter Server entre sí. Consulte Particiones de red . Cuando se produce una partición, la protección de Fault Tolerance puede degradarse.

En un clúster de vSphere HA particionado con Fault Tolerance, la máquina virtual principal (o su máquina virtual secundaria) podría terminar en una partición administrada por un host principal que no es responsable de la máquina virtual. Cuando se necesita una conmutación por error, la máquina virtual secundaria se reinicia solo si la máquina virtual principal estaba en una partición administrada por el host principal responsable de ella.

Para asegurar que su red de administración tenga menos probabilidades de experimentar un error que lleve a una partición de la red, siga las recomendaciones en Prácticas recomendadas para redes.

Utilizar almacenes de datos de vSAN

vSphere Fault Tolerance puede utilizar almacenes de datos de vSAN, pero se deben tener en cuenta las siguientes restricciones:

- Las máquinas virtuales principales y secundarias no admiten la mezcla de vSAN y otros tipos de almacenes de datos.
- FT no admite clústeres metro de vSAN.

Para aumentar el rendimiento y la confiabilidad mediante FT con vSAN, también se recomiendan las siguientes condiciones.

- vSAN y FT deben utilizar redes distintas.
- Conserve las máquinas virtuales principales y secundarias en dominios de errores de vSAN distintos.

Fault Tolerance heredado

De manera predeterminada, vSphere Fault Tolerance puede incluir máquinas virtuales SMP con hasta cuatro vCPU. Sin embargo, si su máquina virtual tiene solo una vCPU, puede usar FT heredado para compatibilidad con versiones anteriores. Evite usar FT heredado a menos que sea técnicamente necesario.

Para usar Fault Tolerance heredado, debe configurar una opción avanzada para la máquina virtual. Después de concluir esta configuración, la máquina virtual con FT heredado es diferente de cierta forma respecto de otras máquinas virtuales con vSphere FT.

Diferencias de las máquinas virtuales que usan FT heredado

Las máquinas virtuales que usan vSphere FT y las máquinas virtuales que utilizan FT heredado se diferencian de varias formas.

Tabla 3-2. Diferencias entre FT heredado y vSphere FT

	FT heredado	vSphere FT
Tablas de páginas extendidas/ Indexación de virtualización rápida (EPT/RVI)	No compatible	Obligatorio
IPv6	No compatibles para NIC de registro de FT heredado.	Compatible para NIC de registro de vSphere FT.
DRS	Totalmente compatible para la colocación inicial, el equilibrio de carga y la compatibilidad con modo de mantenimiento.	Solo se admite la colocación de encendido de máquinas virtuales secundarias y el modo de mantenimiento.
API de vStorage - copias de seguridad para protección de datos	No compatible	Compatible
Archivos .vmdk de disco grueso puestos a cero	Obligatorio	No se requiere debido a que vSphere FT es compatible con todos los tipos de archivo de disco, incluidos los gruesos y los finos.
Redundancia de .vmdk	Solo una copia	Las máquinas virtuales principales y las secundarias siempre mantienen copias independientes que se pueden colocar en diferentes almacenes de datos para aumentar la redundancia.
Ancho de banda de la NIC	Se recomienda una NIC dedicada de 1 Gb	Se recomienda una NIC dedicada de 10 Gb

Tabla 3-2. Diferencias entre FT heredado y vSphere FT (continuación)

	FT heredado	vSphere FT
Compatibilidad de CPU y host	Requiere versiones idénticas de modelo y familia de CPU y versiones casi idénticas de vSphere en los hosts.	Las CPU deben ser compatibles con vSphere vMotion o EVC. Las versiones de vSphere en los hosts deben ser compatibles con vSphere vMotion.
Activar FT en máquina virtual en ejecución	No siempre es compatible. Puede que primero necesite apagar la máquina virtual.	Compatible
Storage vMotion	Compatible solo en máquinas virtuales apagadas. vCenter Server desactiva automáticamente FT antes de realizar una acción de Storage vMotion y activa FT nuevamente una vez que finaliza la acción de Storage vMotion.	No compatible. El usuario debe desactivar vSphere FT para la máquina virtual antes de realizar la acción de Storage vMotion y volver a activar vSphere FT.
Controladores de redes de vlance	No compatible	Compatible

Requisitos adicionales para FT heredado

Además de las diferencias que se indican para FT heredado, también tiene los siguientes requisitos únicos.

- Los hosts ESXi deben tener acceso a los mismos almacenes de datos y redes de máquina virtual.
- Las máquinas virtuales deben estar almacenadas en archivos RDM virtuales o archivos de disco de máquina virtual (VMDK) que tienen aprovisionamiento grueso. Si una máquina virtual está almacenada en un archivo de VMDK que tiene aprovisionamiento fino y se hace un intento de usar Fault Tolerance, aparece un mensaje. El mensaje indica que se debe convertir el archivo de VMDK. Para realizar la conversión, debe apagar la máquina virtual.
- Los hosts deben tener procesadores del grupo de procesadores compatibles con vSphere FT. Compruebe que los procesadores de los hosts sean compatibles entre sí.
- El host que es compatible con la máquina virtual secundaria debe tener un procesador que sea compatible con Fault Tolerance y que tenga la misma familia o el mismo modelo de CPU que el host que admite la máquina virtual principal.
- Cuando actualice hosts que contengan máquinas virtuales con Fault Tolerance, compruebe que las máquinas virtuales principales y secundarias sigan ejecutándose en los hosts con el mismo número de versión de FT o número de compilación de host. Este requisito se aplica a hosts anteriores a ESX/ESXi 4.1.

  Nota Si designó una máquina virtual para que usara FT heredado antes de actualizar los hosts en el clúster, esa máquina virtual sigue utilizando FT heredado después de la actualización del host.

Actualización de hosts implicados con FT heredado

Para actualizar sus hosts a la versión vSphere 6.5 o posterior, debe apagar el FT heredado en todas las máquinas virtuales afectadas o mover esas máquinas virtuales a otros hosts. Si no realiza esta preparación para la actualización, VMware vSphere Update Manager bloquea la actualización.

La versión 6.5 o posterior de vCenter Server puede administrar las máquinas virtuales con FT heredado existentes, pero no se pueden crear máquinas virtuales con FT heredado en hosts cuya versión sea anterior a la 6.5. Las siguientes operaciones de vSphere FT se pueden realizar en este escenario:

- Suspender o reanudar FT
- Probar conmutación por error
- Reiniciar máquina secundaria
- Migrar máquina secundaria
- Apagar FT

Nota Las máquinas virtuales con FT heredado pueden existir solo en hosts ESXi que se ejecutan en versiones de vSphere anteriores a la 6.5.

---

vCenter High Availability

4

vCenter High Availability (vCenter HA) protege vCenter Server Appliance de los errores de host y de hardware. La arquitectura activa-pasiva de la solución también puede ayudar a reducir en gran medida el tiempo de inactividad cuando realiza una revisión de vCenter Server Appliance.

Después de una configuración de red, cree un clúster de tres nodos que tenga nodos activos, pasivos y testigo. Existen distintas rutas de acceso de configuración disponibles. Su elección depende de la configuración actual.

Procedimiento

1 Planificar la implementación de vCenter HA

   Antes de configurar vCenter HA, es necesario considerar varios factores. En la implementación de vCenter Server Appliance se puede utilizar una instancia interna o externa de Platform Services Controller. Para una implementación de entorno no virgen con componentes que utilizan distintas versiones de vSphere, se requieren distintas consideraciones que para una implementación de entorno virgen, la cual incluye solo componentes de vSphere 6.5. Los requisitos de recursos y software, así como la configuración de redes, también son factores que deben considerarse detenidamente.

2 Configurar la red

   Independientemente de la opción de implementación y la jerarquía de inventario que se seleccionen, es necesario configurar la red antes de iniciar la configuración. Para establecer las bases de la red de vCenter HA, se debe agregar un grupo de puertos a cada host ESXi y agregar una NIC virtual a la instancia de vCenter Server Appliance que se convertirá en el nodo activo.

3 Configurar vCenter HA con la opción básica

   Cuando utiliza la opción básica, el asistente de vCenter HA crea y configura un segundo adaptador de red en vCenter Server Appliance, clona el nodo activo y configura la red de vCenter HA.

4 Configurar vCenter HA con la opción avanzada

   Si configura el clúster de vCenter HA con la opción avanzada, tiene más control sobre el entorno y no debe cumplir algunos de los requisitos previos para la configuración básica. Sin embargo, usted es responsable de agregar una segunda NIC en vCenter Server Appliance, de clonar el nodo activo en los nodos pasivo y testigo, y de configurar los clones.

5 Administrar la configuración de vCenter HA

Después de configurar el clúster de vCenter HA, puede realizar tareas de administración. Entre estas tareas se incluyen el reemplazo de certificados, el reemplazo de claves SSH y la configuración de SNMP. También puede editar la configuración de clústeres para habilitar y deshabilitar vCenter HA, entrar a modo de mantenimiento y eliminar la configuración de clústeres.

6 Solucionar problemas del entorno de vCenter HA

En caso de que haya problemas en el entorno, puede solucionarlos. La tarea que se debe realizar depende de los síntomas del error. Para obtener información adicional sobre la solución de problemas, consulte el sistema de la base de conocimientos de VMware.

7 Aplicar revisiones en un entorno de vCenter High Availability

Es posible aplicar una revisión en una instancia de vCenter Server Appliance que se encuentra en un clúster de vCenter High Availability mediante la utilidad **`software-packages`** disponible en el shell de vCenter Server Appliance.

Planificar la implementación de vCenter HA

Antes de configurar vCenter HA, es necesario considerar varios factores. En la implementación de vCenter Server Appliance se puede utilizar una instancia interna o externa de Platform Services Controller. Para una implementación de entorno no virgen con componentes que utilizan distintas versiones de vSphere, se requieren distintas consideraciones que para una implementación de entorno virgen, la cual incluye solo componentes de vSphere 6.5. Los requisitos de recursos y software, así como la configuración de redes, también son factores que deben considerarse detenidamente.

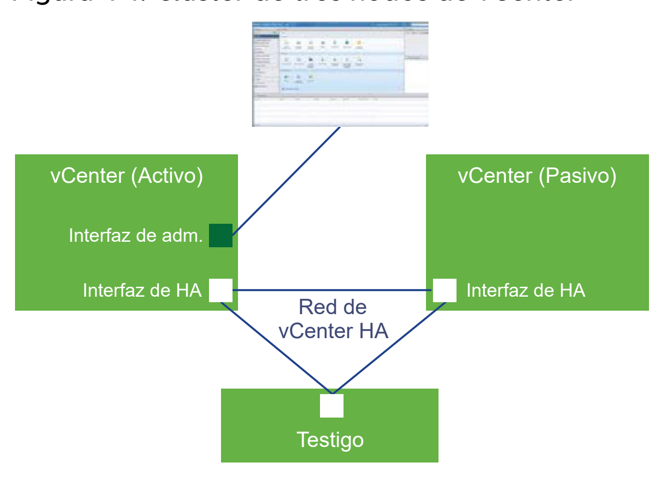
Descripción general de la arquitectura de vCenter

Un clúster de vCenter HA consiste en tres instancias de vCenter Server Appliance. La primera instancia, inicialmente usada como el nodo activo, se clona dos veces para un nodo pasivo y un nodo testigo. En conjunto, los tres nodos ofrecen una solución de conmutación por error activa-pasiva.

La implementación de cada uno de los nodos en una instancia de ESXi diferente protege contra errores de hardware. Agregar los tres hosts ESXi al clúster de DRS puede brindar protección adicional para el entorno.

Cuando se termine la configuración de vCenter HA, solo el nodo activo tiene una interfaz de administración activa (IP pública). Los tres nodos se comunican en una red privada denominada red de vCenter HA que se configura como parte de la configuración. El nodo activo y el nodo pasivo no duplican datos en forma continua.

Figura 4-1. Clúster de tres nodos de vCenter



Los tres nodos son necesarios para el funcionamiento de esta función. Compare las responsabilidades de los nodos.

Tabla 4-1. Nodos de vCenter HA

Nodo	Descripción
activa	■ Ejecuta la instancia activa de vCenter Server Appliance. ■ Usa una dirección IP pública para la interfaz de administración. ■ Utiliza la red de vCenter HA para duplicar datos en el nodo pasivo. ■ Utiliza la red de vCenter HA para comunicarse con el nodo testigo.
Pasiva	■ Inicialmente, es un clon del nodo activo. ■ Recibe constantemente actualizaciones y sincroniza el estado con el nodo activo en la red de vCenter HA. ■ Si se produce un error, toma automáticamente la función del nodo activo.
Testigo	■ Es un clon liviano del nodo activo. ■ Proporciona cuórum para proteger contra situaciones de cerebro dividido.

Requisitos de hardware y software de vCenter HA

Antes de configurar vCenter HA, asegúrese de que tener suficiente memoria, CPU y recursos de almacén de datos, así como de utilizar versiones de vCenter Server y ESXi que admitan vCenter HA.

El entorno debe cumplir con los siguientes requisitos.

Tabla 4-2. Requisitos de vCenter HA

Componente	Requisitos
ESXi	■ Se requiere ESXi 5.5 o posterior. ■ Se recomienda el uso de tres hosts. Posteriormente, cada nodo de vCenter HA puede ejecutarse en un host distinto para lograr una mejor protección. ■ Se recomienda usar VMware DRS para proteger el conjunto de hosts. En ese caso, se requiere un mínimo de tres hosts ESXi.
Management vCenter Server (si se usa)	El entorno puede incluir un sistema de administración de vCenter Server o puede configurar vCenter Server Appliance para administrar el host ESXi en el que se ejecuta (vCenter Server autoadministrado). ■ Se requiere vCenter Server 5.5 o posterior.
vCenter Server Appliance	■ Se requiere vCenter Server 6.5. ■ Se requiere un tamaño de implementación pequeño (4 CPU y 16 GB de RAM) o más grande para cumplir el RTO. No utilice implementaciones muy pequeñas en entornos de producción. ■ vCenter HA se admite y se pone a prueba con almacenes de datos de VMFS, NFS y vSAN. ■ Asegúrese de tener suficiente espacio de disco para recopilar y almacenar los paquetes de soporte para los tres nodos del nodo activo. Consulte Recopilar paquetes de soporte para un nodo de vCenter HA.
Conectividad de red	■ La latencia de red de vCenter HA entre los nodos activo, pasivo y testigo debe ser inferior a 10 ms. ■ La red de vCenter HA debe estar en una subred diferente a la red de administración.
Licencias necesarias para vCenter HA	■ vCenter HA requiere una única licencia de vCenter Server. ■ vCenter HA requiere una licencia estándar.

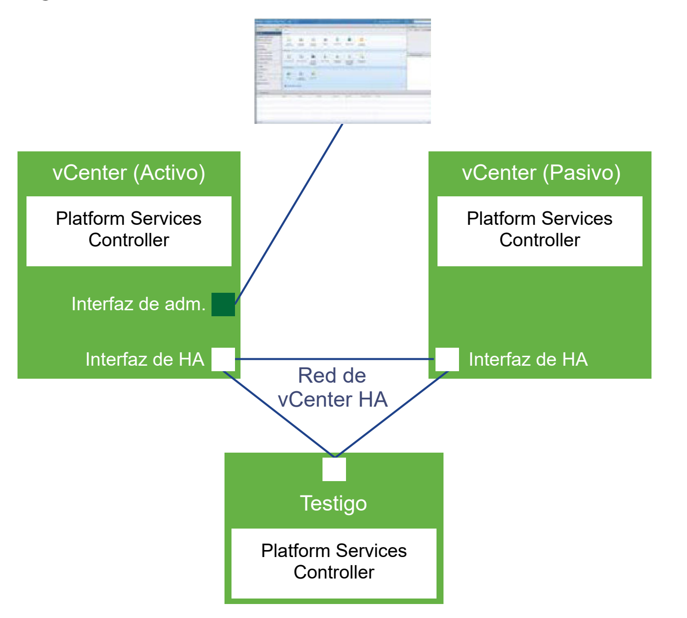
Opciones de implementación de vCenter HA

Se puede configurar el entorno de vCenter HA con una instancia de Platform Services Controller integrada o una instancia de Platform Services Controller externa. Si decide utilizar una instancia de Platform Services Controller externa, puede colocarla detrás de un equilibrador de carga para protegerla en caso de que se produzca un error en Platform Services Controller.

vCenter HA con una instancia de Platform Services Controller integrada

Cuando se utiliza vCenter HA con una instancia de Platform Services Controller integrada, la configuración del entorno es la siguiente.

Figura 4-2. vCenter HA con una instancia de Platform Services Controller integrada



1 El usuario aprovisiona vCenter Server Appliance con una instancia de Platform Services Controller integrada.

2 Se produce la clonación de una instancia de vCenter Server Appliance a un nodo pasivo y testigo.

   - En una configuración básica, la configuración crea y configura los clones.
   - En una configuración avanzada, el usuario crea y configura los clones.

3 Como parte del proceso de clonación, también se clonan Platform Services Controller y todos sus servicios.

4 Una vez que la configuración se completó, vCenter HA realiza una replicación para garantizar que el nodo pasivo esté sincronizado con el nodo activo. La replicación de nodo activo a nodo pasivo incluye datos de Platform Services Controller.

5 Una vez que la configuración se completó, vCenter Server Appliance queda protegido por vCenter HA. En caso de que se produzca una conmutación por error, Platform Services Controller y todos sus servicios quedan disponibles en el nodo pasivo.

vCenter HA con una instancia de Platform Services Controller externa

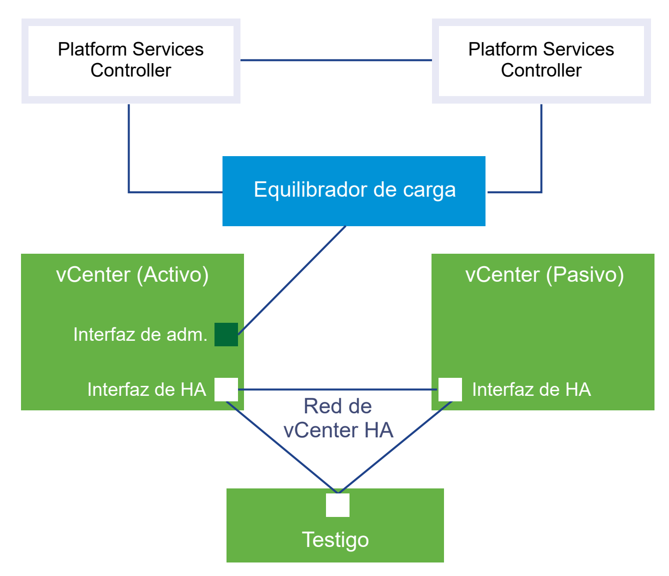
Cuando se utiliza vCenter HA con una instancia de Platform Services Controller externa, se debe configurar un equilibrador de carga externo para proteger Platform Services Controller. Si una instancia de Platform Services Controller no está disponible, el equilibrador de carga dirige vCenter Server Appliance a una instancia de Platform Services Controller distinta.

En los siguientes artículos de la base de conocimientos de VMware se trata la configuración de la instancia de Platform Services Controller externa.

- 2147014: Configurar Netscaler Load Balancer para el uso con vSphere Platform Services Controller (PSC) 6.5
- 2147038: Configurar F5 BIG-IP Load Balancer para el uso con vSphere Platform Services Controller (PSC) 6.5
- 2147046: Configurar NSX Edge Load Balancer para el uso con vSphere Platform Services Controller (PSC) 6.5

La configuración del entorno es la siguiente.

Figura 4-3. vCenter HA con una instancia de Platform Services Controller externa



1 El usuario configura por lo menos dos instancias de Platform Services Controller externas. Estas instancias replican información de vCenter Single Sign-On y otra información de Platform Services Controller, por ejemplo, las licencias.

2 Durante el aprovisionamiento de vCenter Server Appliance, el usuario selecciona una instancia de Platform Services Controller externa.

3 El usuario configura vCenter Server Appliance a fin de que apunte a un equilibrador de carga que proporcione alta disponibilidad para Platform Services Controller.

4 El usuario o la configuración básica clonan la primera instancia de vCenter Server Appliance para crear el nodo pasivo y el nodo testigo.

5 Como parte del proceso de clonación, también se clonan la información sobre la instancia de Platform Services Controller externa y el equilibrador de carga.

6 Una vez que la configuración se completó, vCenter Server Appliance queda protegido por vCenter HA.

7 Si la instancia de Platform Services Controller no está disponible, el equilibrador de carga redirige las solicitudes para la autenticación u otros servicios para la segunda instancia de Platform Services Controller.

Descripción general del flujo de trabajo de la configuración

Puede seleccionar la opción de configuración básica o avanzada. La opción básica crea automáticamente los nodos pasivo y testigo como parte de la configuración de vCenter HA. Si elige la opción avanzada, deberá clonar manualmente el nodo activo para crear los nodos pasivo y testigo.

La opción de configuración que seleccione dependerá del entorno. Los requisitos de la configuración básica son más estrictos, pero el proceso de configuración está más automatizado. Se puede emplear la configuración avanzada si el entorno cumple con los requisitos de hardware y software, y si ofrece más flexibilidad. No obstante, la configuración avanzada requiere la creación y la configuración de los clones del nodo activo.

Flujo de trabajo de la configuración básica

La configuración básica clona automáticamente el nodo activo. Debe cumplir con uno de los siguientes requisitos para realizar la configuración básica.

- La instancia de vCenter Server Appliance que se convertirá en el nodo activo administra su propio host ESXi y su propia máquina virtual. Esta configuración a veces se denomina instancia de vCenter Server autoadministrada.
- La instancia de vCenter Server Appliance es administrada por otra instancia de vCenter Server (vCenter Server de administración) y ambas instancias de vCenter Server se deben encontrar en el mismo dominio de vCenter Single Sign-On. Eso significa que ambas utilizan una instancia de Platform Services Controller externa y ambas ejecutan vSphere 6.5.

Si cumple con los requisitos, el flujo de trabajo de la configuración básica es el siguiente.

1 El usuario implementa la primera instancia de vCenter Server Appliance, que se convertirá en el nodo activo.

2 El usuario agrega una segunda red (grupo de puertos) para el tráfico de vCenter HA en cada host ESXi.

3 El usuario inicia la configuración de vCenter HA, selecciona la opción Básica y proporciona las direcciones IP, el clúster o host ESXi de destino y el almacén de datos para cada clon.

4 El sistema clona el nodo activo y crea un nodo pasivo exactamente con la misma configuración, incluido el mismo nombre de host.

5 A continuación, el sistema vuelve a clonar el nodo activo y crea un nodo testigo más ligero.

6 El sistema configura la red de vCenter HA donde se comunican los tres nodos, por ejemplo, mediante el intercambio de latidos y otro tipo de información.

Para obtener instrucciones detalladas, consulte Configurar vCenter HA con la opción básica.

Flujo de trabajo de la configuración avanzada

Si no puede seleccionar la opción Básica o si desea tener un mayor control de la implementación, puede realizar una configuración avanzada. Si elige esta opción, deberá encargarse de clonar el nodo activo como parte de la configuración de vCenter HA. Si selecciona esta opción y elimina la configuración de vCenter HA más adelante, será responsable de eliminar los nodos que creó.

El flujo de trabajo de la opción avanzada es el siguiente.

1 El usuario implementa la primera instancia de vCenter Server Appliance, que se convertirá en el nodo activo.
2 El usuario agrega una segunda red (grupo de puertos) para el tráfico de vCenter HA en cada host ESXi.
3 El usuario agrega un segundo adaptador de red (NIC) al nodo activo.
4 El usuario inicia sesión en vCenter Server Appliance (nodo activo) con vSphere Web Client.
5 El usuario inicia la configuración de vCenter HA, selecciona la opción avanzada y proporciona la dirección IP y la información de subred de los nodos pasivo y testigo. Como alternativa, el usuario puede anular las direcciones IP de administración de la conmutación por error.
6 El usuario inicia sesión en la instancia de vCenter Server de administración y crea dos clones de vCenter Server Appliance (nodo activo).
7 A continuación, regresa al asistente de configuración en vCenter Server Appliance y completa el proceso de configuración.
8 El sistema configura la red de vCenter HA en la que los tres nodos intercambian latidos e información de replicación.
9 La instancia de vCenter Server Appliance está protegida por vCenter HA.

Consulte Configurar vCenter HA con la opción avanzada para obtener detalles.

Configurar la red

Independientemente de la opción de implementación y la jerarquía de inventario que se seleccionen, es necesario configurar la red antes de iniciar la configuración. Para establecer las bases de la red de vCenter HA, se debe agregar un grupo de puertos a cada host ESXi y agregar una NIC virtual a la instancia de vCenter Server Appliance que se convertirá en el nodo activo.

Una vez completada la configuración, el clúster de vCenter HA incluirá dos redes: la red de administración en la primera NIC virtual y la red de vCenter HA en la segunda NIC virtual.

Red de administración

La red de administración atiende las solicitudes de los clientes (IP pública). Las direcciones IP de la red de administración deben ser estáticas.

Red de vCenter HA

La red de vCenter HA conecta los nodos activo, pasivo y testigo, y replica el estado del dispositivo. También supervisa los latidos.

- Las direcciones IP de la red de vCenter HA para los nodos activo, pasivo y testigo deben ser estáticas.
- La red de vCenter HA debe estar en una subred diferente a la red de administración. Los tres nodos pueden estar en la misma subred o en subredes diferentes.
- La latencia de red entre los nodos activo, pasivo y testigo debe ser inferior a 10 milisegundos.
- No se debe agregar una entrada de puerta de enlace predeterminada para la red de clúster.

Requisitos previos

- Se implementa la instancia de vCenter Server Appliance que se convertirá posteriormente en el nodo activo.
- Es posible acceder y adquirir privilegios para modificar esa instancia de vCenter Server Appliance y el host ESXi en el cual se ejecuta.
- Durante la configuración de la red, se requieren direcciones IP estáticas para la red de administración. Las direcciones de las redes de administración y de clúster deben ser IPv4 o IPv6. No pueden ser mixtas.

Procedimiento

1 Inicie sesión en la instancia de vCenter Server de administración y busque el host ESXi donde se ejecuta el nodo activo.

2 Agregue un grupo de puertos al host ESXi.

   Este grupo de puertos se puede tomar de un conmutador virtual existente o, si se desea mejorar el aislamiento de la red, se puede crear un conmutador virtual nuevo. Debe estar en una subred diferente a la red de administración en Eth0.

3 Si el entorno contiene los tres hosts ESXi recomendados, agregue el grupo de puertos a cada uno de los hosts.

Pasos siguientes

Los pasos a seguir dependerán del tipo de configuración seleccionada.

- En una configuración básica, el asistente creará la NIC virtual de vCenter HA en cada clon y configurará la red de vCenter HA. Una vez finalizada la configuración, la red de vCenter HA estará disponible para la replicación y el tráfico de latidos.
- En una configuración avanzada:
  - Primero se debe crear y configurar una segunda NIC en el nodo activo. Consulte Crear y configurar una segunda NIC en vCenter Server Appliance.

- Al realizar la configuración, el asistente solicitará las direcciones IP para los nodos pasivo y testigo.
- El asistente solicitará clonar el nodo activo. Se deberán configurar otras opciones de red como parte del proceso de clonación.

Consulte Configurar vCenter HA con la opción avanzada.

Configurar vCenter HA con la opción básica

Cuando utiliza la opción básica, el asistente de vCenter HA crea y configura un segundo adaptador de red en vCenter Server Appliance, clona el nodo activo y configura la red de vCenter HA.

Requisitos previos

- Implemente la instancia de vCenter Server Appliance que desea utilizar como nodo activo inicial.
  - El dispositivo vCenter Server Appliance debe tener una dirección IP estática.
  - SSH debe estar habilitado en vCenter Server Appliance.
- Compruebe que el entorno cumpla con uno de los siguientes requisitos.
  - La instancia de vCenter Server Appliance que se convertirá en el nodo activo administra su propio host ESXi y su propia máquina virtual. Esta configuración a veces se denomina instancia de vCenter Server autoadministrada.
  - O bien, la instancia de vCenter Server Appliance está administrada por otro vCenter Server (vCenter Server de administración) y los dos dispositivos están en el mismo dominio de vCenter Single Sign-On. Eso significa que ambos utilizan una instancia de Platform Services Controller externa y ambos ejecutan vSphere 6.5.

  Si el entorno no cumple con uno de estos requisitos, realice una configuración avanzada. Consulte Configurar vCenter HA con la opción avanzada.
- Configure la infraestructura para la red de vCenter HA. Consulte Configurar la red.
- Determine qué direcciones IP estáticas se deben utilizar para los dos nodos de vCenter Server Appliance que se convertirán en nodo pasivo y nodo testigo.

Procedimiento

1. Inicie sesión en el nodo activo con vSphere Web Client.
2. Haga clic con el botón derecho en el objeto de vCenter Server del inventario y seleccione **Configuración de vCenter HA**.
3. Haga clic en **Configurar**.
4. Seleccione la opción de configuración **Básica** y haga clic en **Siguiente**.

   Esta opción está disponible solo si el entorno cumple con los requisitos previos para esta opción.

5 Especifique la dirección IP, la máscara de subred del nodo activo y el grupo de puertos para conectarse a la red de vCenter HA y, a continuación, haga clic en **Siguiente**.

6 Proporcione la dirección IP de la red y la máscara de subred de vCenter HA para los nodos pasivo y testigo y, a continuación, haga clic en **Siguiente**.

   El asistente de configuración necesita las direcciones para crear la red de vCenter HA y conectar los tres nodos.

7 (opcional) Haga clic en **Configuración avanzada** si desea anular la dirección IP de administración de conmutación por error para el nodo pasivo.

8 Repase la información de los nodos pasivo y testigo, haga clic en **Editar** para realizar cambios y, a continuación, haga clic en **Siguiente**.

   Si no utiliza un clúster de DRS, seleccione hosts y almacenes de datos diferentes para los nodos pasivo y testigo siempre que sea posible.

9 Haga clic en **Finalizar**.

Resultados

Se crean los nodos pasivo y testigo. Cuando finaliza la configuración de vCenter HA, vCenter Server Appliance posee protección de alta disponibilidad.

Pasos siguientes

Consulte Administrar la configuración de vCenter HA para acceder a una lista de tareas de administración de clústeres.

Configurar vCenter HA con la opción avanzada

Si configura el clúster de vCenter HA con la opción avanzada, tiene más control sobre el entorno y no debe cumplir algunos de los requisitos previos para la configuración básica. Sin embargo, usted es responsable de agregar una segunda NIC en vCenter Server Appliance, de clonar el nodo activo en los nodos pasivo y testigo, y de configurar los clones.

Procedimiento

1 Crear y configurar una segunda NIC en vCenter Server Appliance

   Antes de poder comenzar con la configuración avanzada, debe crear y configurar una segunda NIC en la instancia de vCenter Server Appliance que se convertirá en el nodo activo. Esta NIC se utilizará para el tráfico de vCenter HA. Debe realizar esta tarea después de configurar la red, pero antes de iniciar el proceso de configuración.

2 Iniciar el proceso de configuración avanzada

   Después de configurar la red y agregar una segunda NIC a vCenter Server Appliance, puede iniciar el proceso de configuración de vCenter HA.

3 Crear y configurar los clones en el nodo activo

Como parte de la configuración avanzada, es necesario clonar el nodo activo para crear los nodos pasivo y testigo. No cierre el asistente Configurar vCenter HA durante la ejecución de las tareas de clonación.

4 Completar la configuración avanzada de vCenter HA

Una vez creados los nodos pasivo y testigo, regrese al asistente de configuración en el nodo activo para completar la configuración.

Crear y configurar una segunda NIC en vCenter Server Appliance

Antes de poder comenzar con la configuración avanzada, debe crear y configurar una segunda NIC en la instancia de vCenter Server Appliance que se convertirá en el nodo activo. Esta NIC se utilizará para el tráfico de vCenter HA. Debe realizar esta tarea después de configurar la red, pero antes de iniciar el proceso de configuración.

Requisitos previos

- Configure la infraestructura para la red de vCenter HA. Consulte Configurar la red.
- Implemente la instancia de vCenter Server Appliance que desea utilizar como nodo activo inicial.
  - La instancia de vCenter Server Appliance debe tener una dirección IP estática asignada a un FQDN.
  - SSH debe estar habilitado en vCenter Server Appliance.

Procedimiento

1 Inicie sesión en la instancia de vCenter Server de administración con vSphere Web Client.

2 Seleccione la máquina virtual de vCenter Server Appliance (nodo activo), agregue un segundo adaptador de red y asócielo al grupo de puertos de vCenter HA que creó.

3 Inicie sesión en la instancia de vCenter Server Appliance que se convertirá en el nodo activo inicial, directamente.

Interfaz	Acción
vCenter Server Appliance	Vaya a https://*appliance-IP-address-or-FQDN*:5480
vSphere Web Client	a Vaya a https://*appliance-IP-address-or-FQDN*/vsphere-client b Seleccione **Administración > Configuración del sistema**.

4 Configure las opciones de IP del segundo adaptador de red.

Iniciar el proceso de configuración avanzada

Después de configurar la red y agregar una segunda NIC a vCenter Server Appliance, puede iniciar el proceso de configuración de vCenter HA.

Requisitos previos

- Implemente la instancia de vCenter Server Appliance que desea utilizar como nodo activo inicial.
  - La instancia de vCenter Server Appliance debe tener una dirección IP estática asignada a un FQDN.
  - SSH debe estar habilitado en vCenter Server Appliance.
- Configure la red. Consulte Configurar la red.
- Determine qué direcciones IP estáticas se deben utilizar para los dos nodos de vCenter Server Appliance que se convertirán en nodo pasivo y nodo testigo.

Procedimiento

1 Inicie sesión en el nodo activo con vSphere Web Client.

2 Haga clic con el botón derecho en el objeto de vCenter Server del inventario y seleccione **Configuración de vCenter HA**.

3 Haga clic en **Configurar**.

4 Seleccione la opción **Configuración avanzada** y haga clic en **Siguiente**.

5 Proporcione la dirección IP y la máscara de subred para los nodos pasivo y testigo y, a continuación, haga clic en **Siguiente**.

   Debe especificar estas direcciones IP ahora, aunque los nodos aún no existan. No podrá cambiar estas direcciones IP después de hacer clic en **Siguiente**.

6 (opcional) Haga clic en **Configuración avanzada** si desea anular la dirección IP de administración de conmutación por error para el nodo pasivo.

7 Deje abierto el asistente y realice las tareas de clonación.

Pasos siguientes

Crear y configurar los clones en el nodo activo.

Crear y configurar los clones en el nodo activo

Como parte de la configuración avanzada, es necesario clonar el nodo activo para crear los nodos pasivo y testigo. No cierre el asistente Configurar vCenter HA durante la ejecución de las tareas de clonación.

Procedimiento

1 Inicie sesión en la instancia de vCenter Server de administración, haga clic con el botón derecho en la máquina virtual de vCenter Server Appliance (nodo activo) y seleccione **Clonar > Clonar a máquina virtual**.

2 Introduzca los siguientes valores para el primer clon que se convertirá en el nodo pasivo.

Opción	Valor
Nombre de la máquina virtual nueva	El nombre del nodo pasivo. Por ejemplo, vcsa-peer.
Seleccionar recurso informático **Seleccionar almacenamiento**	Si es posible, procure que el almacén de datos y el host de destino sean diferentes a los del nodo activo.
Opciones de clonación	Seleccione las casillas **Personalizar sistema operativo** y **Encender máquina virtual tras la creación**, y haga clic en el icono Nueva especificación de personalización en la página siguiente. En el asistente Nueva especificación de personalización que se abrirá, especifique lo siguiente. a Utilice el mismo nombre de host que en el nodo activo. b Asegúrese de que la zona horaria sea coherente con el nodo activo. Mantenga el mismo Código de área/ubicación con UTC que en el nodo activo. Si no especificó el Código de área/ubicación con UTC al configurar el nodo activo, elija Londres en Código de área/ubicación durante la clonación. Londres tiene un desplazamiento de 0.00, por lo que mantiene el reloj en UTC sin ningún desplazamiento. c En la página Configurar red, especifique la configuración de IP para NIC1 y NIC2, que conducen a la interfaz de administración y la interfaz de vCenter HA. Deje en blanco la puerta de enlace predeterminada de NIC2.

3 Una vez creado el primer clon, vuelva a clonar el nodo activo para crear el nodo testigo.

Opción	Valor
Nombre de la máquina virtual nueva	El nombre del nodo testigo. Por ejemplo, vcsa-witness.
Seleccionar recurso informático **Seleccionar almacenamiento**	Si es posible, procure que el almacén de datos y el host de destino sean diferentes a los de los nodos activo y pasivo.
Opciones de clonación	Seleccione las casillas Personalizar sistema operativo y Encender máquina virtual tras la creación, y haga clic en el icono Nueva especificación de personalización en la página siguiente. En el asistente Nueva especificación de personalización que se abrirá, especifique lo siguiente. a Use el nombre de host que desee. b Asegúrese de que la zona horaria sea coherente con el nodo activo. Mantenga el mismo Código de área/ubicación con UTC que en el nodo activo. Si no especificó el Código de área/ubicación con UTC al configurar el nodo activo, elija Londres en Código de área/ubicación durante la clonación. Londres tiene un desplazamiento de 0.00, por lo que mantiene el reloj en UTC sin ningún desplazamiento. c En la página Configurar red, especifique la configuración de IP para NIC2, que conduce a la interfaz de vCenter HA. Deje en blanco la puerta de enlace predeterminada de NIC2.

4 Asegúrese de que el proceso de clonación se complete y que las máquinas virtuales se enciendan.

Pasos siguientes

Regrese al asistente de vCenter HA en el nodo activo para completar la configuración. Consulte Completar la configuración avanzada de vCenter HA.

Completar la configuración avanzada de vCenter HA

Una vez creados los nodos pasivo y testigo, regrese al asistente de configuración en el nodo activo para completar la configuración.

Requisitos previos

Complete el proceso de clonación del nodo activo en un nodo pasivo y un nodo testigo.

Procedimiento

1 Regrese al asistente de configuración y haga clic en **Finalizar**.

2 Espere a que finalice la configuración de vCenter HA.

Administrar la configuración de vCenter HA

Después de configurar el clúster de vCenter HA, puede realizar tareas de administración. Entre estas tareas se incluyen el reemplazo de certificados, el reemplazo de claves SSH y la configuración de SNMP. También puede editar la configuración de clústeres para habilitar y deshabilitar vCenter HA, entrar a modo de mantenimiento y eliminar la configuración de clústeres.

- Configurar capturas de SNMP

  Se pueden configurar capturas Simple Network Management Protocol (SNMP) para recibir notificaciones de SNMP para el clúster de vCenter HA.

- Configurar el entorno para usar certificados personalizados

  El certificado SSL de máquina de cada nodo se utiliza para la comunicación de administración de clústeres y el cifrado del tráfico de replicación. Si desea utilizar certificados personalizados, debe eliminar la configuración de vCenter HA, eliminar los nodos pasivo y testigo, aprovisionar el nodo activo con el certificado personalizado y volver a configurar el clúster.

- Administrar las claves SSH de vCenter HA

  vCenter HA utiliza claves SSH para la autenticación sin contraseña entre los nodos activo, pasivo y testigo. La autenticación se utiliza para el intercambio de latidos y la replicación de archivos y datos. Para reemplazar las claves SSH en los nodos de un clúster de vCenter HA, deshabilite el clúster, genere nuevas claves SSH en el nodo activo, transfiera las claves al nodo pasivo y, a continuación, habilite el clúster.

- Iniciar una conmutación por error de vCenter HA

  Se puede iniciar manualmente una conmutación por error y hacer que el nodo pasivo se convierta en el nodo activo.

- Editar la configuración del clúster de vCenter HA

  Al editar la configuración de un clúster de vCenter HA, se puede deshabilitar o habilitar el clúster, colocarlo en modo de mantenimiento o eliminarlo.

- Realizar operaciones de restauración y copia de seguridad

  Para mayor seguridad, puede realizar una copia de seguridad del nodo activo en el clúster de vCenter HA. A continuación, puede restaurar el nodo en caso de que se produzca un error grave.

- Eliminar una configuración de vCenter HA

  Puede eliminar una configuración de vCenter HA de vSphere Web Client. Si está usando la configuración avanzada o si no puede detectar alguno de los nodos, es posible que tenga que realizar pasos de limpieza adicionales.

- Reiniciar todos los nodos de vCenter HA

  Si debe desconectar y reiniciar todos los nodos del clúster, debe seguir un orden de apagado específico para evitar que el nodo pasivo asuma la función de nodo activo.

- Cambiar el entorno del dispositivo

  Cuando se implementa una instancia de vCenter Server Appliance, debe seleccionar un entorno. Para vCenter HA, se admiten los tamaños pequeño, mediano, grande y extragrande para entornos de producción. Si necesita más espacio y desea cambiar el entorno, debe eliminar la máquina virtual del nodo pasivo antes de cambiar la configuración.

- Recopilar paquetes de soporte para un nodo de vCenter HA

  La recopilación de un paquete de soporte de todos los nodos de un clúster de vCenter HA ayuda en la solución de problemas.

Configurar capturas de SNMP

Se pueden configurar capturas Simple Network Management Protocol (SNMP) para recibir notificaciones de SNMP para el clúster de vCenter HA.

De forma predeterminada, la versión SNMP de las capturas es la versión 1.

Configurar capturas de SNMP para el nodo Activo y el nodo Pasivo. Para indicar al agente dónde debe enviar las capturas relacionadas, se debe agregar una entrada de destino a la configuración de SNMP.

Procedimiento

1. Inicie sesión en el nodo activo usando la consola de la máquina virtual o SSH.
2. Ejecute el comando `vicfg-snmp`, por ejemplo:

   ```
   vicfg-snmp -t 10.160.1.1@1166/public
   ```

   En este ejemplo, `10.160.1.1` es la dirección de escucha del cliente, `1166` es el puerto de escucha del cliente y `public` es la cadena de comunidad.

3 Para habilitar el agente SNMP (snmpd), ejecute el siguiente comando.

```
vicfg-snmp -e
```

Pasos siguientes

Los siguientes comandos también pueden ser de utilidad.

- Para ver la ayuda completa del comando, ejecute **`vicfg-snmp -h`**.
- Para deshabilitar el agente SNMP, ejecute **`vicfg-snmp -D`**.
- Para mostrar la configuración del agente SNMP, ejecute **`vicfg-snmp -s`**.
- Para restablecer los valores predeterminados de la configuración, ejecute **`vicfg-snmp -r`**.

Configurar el entorno para usar certificados personalizados

El certificado SSL de máquina de cada nodo se utiliza para la comunicación de administración de clústeres y el cifrado del tráfico de replicación. Si desea utilizar certificados personalizados, debe eliminar la configuración de vCenter HA, eliminar los nodos pasivo y testigo, aprovisionar el nodo activo con el certificado personalizado y volver a configurar el clúster.

De ser posible, reemplace los certificados en la instancia de vCenter Server Appliance que se convertirá en el nodo activo antes de clonar el nodo.

Procedimiento

1 Edite la configuración del clúster y seleccione **Quitar**.

2 Elimine el nodo pasivo y el nodo testigo.

3 En el nodo activo, que ahora es una instancia de vCenter Server Appliance independiente, reemplace el certificado SSL de máquina por un certificado personalizado.

   Consulte la documentación de *Administrar Platform Services Controller*.

4 Vuelva a configurar el clúster.

Administrar las claves SSH de vCenter HA

vCenter HA utiliza claves SSH para la autenticación sin contraseña entre los nodos activo, pasivo y testigo. La autenticación se utiliza para el intercambio de latidos y la replicación de archivos y datos. Para reemplazar las claves SSH en los nodos de un clúster de vCenter HA, deshabilite el clúster, genere nuevas claves SSH en el nodo activo, transfiera las claves al nodo pasivo y, a continuación, habilite el clúster.

Procedimiento

1 Edite el clúster y cambie el modo a **Deshabilitado**.

2 Inicie sesión en el nodo activo usando la consola de la máquina virtual o SSH.

3 Habilite el shell de Bash.

```
bash
```

4 Ejecute el siguiente comando para generar las claves SSH nuevas en el nodo activo.

```
/usr/lib/vmware-vcha/scripts/resetSshKeys.py
```

5 Use el SCP para copiar las claves al nodo pasivo y al nodo testigo.

```
scp /vcha/.ssh/*
```

6 Edite la configuración del clúster y establezca el clúster de vCenter HA en **Habilitado**.

Iniciar una conmutación por error de vCenter HA

Se puede iniciar manualmente una conmutación por error y hacer que el nodo pasivo se convierta en el nodo activo.

Un clúster de vCenter HA admite dos tipos de conmutación por error.

Conmutación por error automática

El nodo pasivo intenta tomar la función activa en caso de que se produzca un error en el nodo activo.

Conmutación por error manual

El usuario puede forzar un nodo pasivo para que tome la función activa mediante el uso de la acción Iniciar conmutación por error.

Inicie una conmutación por error manual para solucionar problemas y realizar pruebas.

Procedimiento

1 Inicie sesión en el nodo activo vCenter Server Appliance con vSphere Web Client y haga clic en **Configurar**.

2 En **Configuración**, seleccione **vCenter HA** y haga clic en **Iniciar conmutación por error**.

3 Haga clic en **Sí** para iniciar la conmutación por error.

   Un cuadro de diálogo ofrece la opción de forzar una conmutación por error sin sincronización. En la mayoría de los casos, lo mejor es realizar una sincronización en primer lugar.

4 Después de la conmutación por error, puede verificar que el nodo pasivo tenga la función del nodo activo en vSphere Web Client.

Editar la configuración del clúster de vCenter HA

Al editar la configuración de un clúster de vCenter HA, se puede deshabilitar o habilitar el clúster, colocarlo en modo de mantenimiento o eliminarlo.

El modo de operación de vCenter Server Appliance controla las funcionalidades de conmutación por error y replicación de estado en un clúster de vCenter HA.

El clúster de vCenter HA puede funcionar en uno de los siguientes modos.

Tabla 4-3. Modos de operación del clúster de vCenter HA

Modo	Conmutación por error automática	Conmutación por error manual	Replicación	
Habilitado	Sí	Sí	Sí	Este modo de funcionamiento predeterminado protege vCenter Server Appliance contra los errores de hardware y software mediante la ejecución de una conmutación por error.
Mantenimiento	No	Sí	Sí	Se utiliza para algunas tareas de mantenimiento. Para otras tareas, es necesario deshabilitar vCenter HA.
Deshabilitado	No	No	No	Si los nodos pasivo o testigo se pierden o se recuperan de un error, se puede deshabilitar una configuración de vCenter HA. El nodo activo continúa como instancia de vCenter Server Appliance independiente.

Nota Si el clúster está operando en los modos Mantenimiento o Deshabilitado, un nodo activo puede seguir procesando las solicitudes de los clientes aunque los nodos pasivo y testigo se pierdan o sean inaccesibles.

Requisitos previos

Verifique que el clúster de vCenter HA esté implementado y contenga los nodos activo, pasivo y testigo.

Procedimiento

1 Inicie sesión en el nodo activo vCenter Server Appliance con vSphere Web Client y haga clic en **Configurar**.

2 En **Configuración**, seleccione **vCenter HA** y haga clic en **Editar**.

3 Seleccione una de las opciones.

Opción	Resultado
Habilitar vCenter HA	Se habilita la replicación entre los nodos activo y pasivo. Si el estado del clúster es correcto, el nodo activo está protegido con la conmutación por error automática del nodo pasivo.
Modo de mantenimiento	En modo de mantenimiento, se produce la replicación entre los nodos activo y pasivo. Sin embargo, la conmutación por error automática está deshabilitada.
Deshabilitar vCenter HA	Se deshabilita la replicación y la conmutación por error. Se mantiene la configuración del clúster. Se puede volver a habilitar vCenter HA más tarde.
Eliminar el clúster de vCenter HA	Se elimina el clúster. La replicación y la conmutación por error ya no se proporcionan. El nodo activo continúa funcionando como instancia de vCenter Server Appliance independiente. Consulte Eliminar una configuración de vCenter HA para obtener detalles.

4 Haga clic en Aceptar.

Realizar operaciones de restauración y copia de seguridad

Para mayor seguridad, puede realizar una copia de seguridad del nodo activo en el clúster de vCenter HA. A continuación, puede restaurar el nodo en caso de que se produzca un error grave.

Nota Elimine la configuración del clúster antes de restaurar el nodo activo. No es posible predecir los resultados de la restauración del nodo activo si el nodo pasivo aún se está ejecutando o hay otra configuración del clúster presente.

Requisitos previos

Compruebe la interoperabilidad de vCenter HA y la solución de restauración y copia de seguridad. Una solución es la restauración basada en archivos de vCenter Server Appliance.

Procedimiento

1 Realice una copia de seguridad del nodo activo.

   No realice una copia de seguridad del nodo pasivo y del nodo testigo.

2 Antes de restaurar el clúster, apague y elimine todos los nodos de vCenter HA.

3 Restaure el nodo activo.

   El nodo activo se restaura como instancia de vCenter Server Appliance independiente.

4 Vuelva a configurar la instancia de vCenter HA.

Eliminar una configuración de vCenter HA

Puede eliminar una configuración de vCenter HA de vSphere Web Client. Si está usando la configuración avanzada o si no puede detectar alguno de los nodos, es posible que tenga que realizar pasos de limpieza adicionales.

Procedimiento

1 Inicie sesión en el nodo activo vCenter Server Appliance y haga clic en **Configurar**.

2 En **Configuración**, seleccione **vCenter HA** y haga clic en **Editar**.

3 Seleccione **Eliminar el clúster de vCenter HA**.

 - La configuración del clúster de vCenter HA se elimina de los nodos activo, pasivo y testigo.
 - El nodo activo sigue funcionando como una instancia de vCenter Server Appliance independiente.
 - No se pueden volver a utilizar los nodos pasivo y testigo en una nueva configuración de vCenter HA.
 - Si realizó la configuración con las opciones avanzadas o si los nodos pasivo y testigo no se pueden detectar, debe eliminar estos nodos de manera explícita.
 - Incluso si la segunda NIC virtual se agregó mediante el proceso de configuración, el proceso de eliminación no elimina la NIC virtual.

Reiniciar todos los nodos de vCenter HA

Si debe desconectar y reiniciar todos los nodos del clúster, debe seguir un orden de apagado específico para evitar que el nodo pasivo asuma la función de nodo activo.

Procedimiento

1 Desconecte los nodos en este orden.

 - Nodo pasivo
 - Nodo activo
 - Nodo testigo

2 Reinicie cada nodo.

 Puede reiniciar los nodos en cualquier orden.

3 Compruebe que todos los nodos se unan correctamente al clúster y que el nodo activo anterior vuelva a asumir esa función.

Cambiar el entorno del dispositivo

Cuando se implementa una instancia de vCenter Server Appliance, debe seleccionar un entorno. Para vCenter HA, se admiten los tamaños pequeño, mediano, grande y extragrande para entornos de producción. Si necesita más espacio y desea cambiar el entorno, debe eliminar la máquina virtual del nodo pasivo antes de cambiar la configuración.

Procedimiento

1 Inicie sesión en el nodo activo con vSphere Web Client, edite la configuración del clúster y seleccione **Deshabilitar**.

2 Elimine la máquina virtual del nodo pasivo.

3 Cambie la configuración de vCenter Server Appliance para el nodo activo, por ejemplo, de un entorno pequeño a un entorno mediano.

4 Vuelva a configurar vCenter HA.

Recopilar paquetes de soporte para un nodo de vCenter HA

La recopilación de un paquete de soporte de todos los nodos de un clúster de vCenter HA ayuda en la solución de problemas.

Cuando recopila un paquete de soporte del nodo activo en un clúster de vCenter HA, el sistema se comporta de la siguiente manera.

- Recopila información del paquete de soporte del propio nodo activo.
- Recopila paquetes de soporte de los nodos pasivo y testigo y los coloca en el directorio `commands` del paquete de soporte del nodo activo.

Nota La recopilación de paquetes de soporte de los nodos pasivo y testigo es un mejor esfuerzo, y se produce si es posible acceder a los nodos.

Solucionar problemas del entorno de vCenter HA

En caso de que haya problemas en el entorno, puede solucionarlos. La tarea que se debe realizar depende de los síntomas del error. Para obtener información adicional sobre la solución de problemas, consulte el sistema de la base de conocimientos de VMware.

- La operación de clonación de vCenter HA falla durante la implementación

  Si el proceso de configuración de vCenter HA no crea los clones correctamente, el usuario tiene que resolver ese error de clonación.

- Error en la implementación de vCenter HA

  Los errores de implementación se pueden deber a problemas de configuración, en especial, con la instalación de redes.

- Solucionar problemas de un clúster de vCenter HA degradado

  Para que el estado de un clúster de vCenter HA sea correcto, cada uno de los nodos activo, pasivo y testigo deben estar totalmente operativos y se debe poder acceder a ellos mediante la red del clúster de vCenter HA. Si se produce un error en alguno de los nodos, se considera que el clúster se encuentra en estado degradado.

- Recuperarse de nodos de vCenter HA aislados

  Si los nodos de un clúster de vCenter HA no pueden comunicarse entre sí, el nodo activo deja de procesar las solicitudes de los clientes.

- Resolver errores de conmutación por error

  Cuando un nodo pasivo no se convierte en nodo activo durante una conmutación por error, puede forzar el nodo pasivo para que se convierta en el nodo activo.

- Eventos y alarmas de VMware vCenter® HA

  Si un clúster de vCenter HA está en estado degradado, los eventos y las alarmas muestran errores.

La operación de clonación de vCenter HA falla durante la implementación

Si el proceso de configuración de vCenter HA no crea los clones correctamente, el usuario tiene que resolver ese error de clonación.

Problema

La operación de clonación tiene errores.

Causa

Busque la excepción de clonación. Podría indicar uno de los siguientes problemas.

- Tiene un clúster habilitado para DRS, pero no tiene tres hosts.
- Se perdió la conexión al host o a la base de datos.
- No hay suficiente espacio de disco.
- Existen otros errores de **clonación de máquina virtual**.

Solución

1 Resuelva el error que causó el problema.

2 Quite el clúster y vuelva a iniciar la configuración.

Error en la implementación de vCenter HA

Los errores de implementación se pueden deber a problemas de configuración, en especial, con la instalación de redes.

Problema

Se inicia la configuración de un clúster de vCenter HA y se produce un error. El error tal vez muestre la causa del problema; por ejemplo, quizás vea un mensaje de error en la conexión SSH.

Solución

Si se produce un error de implementación, realice los pasos para resolver los problemas de redes.

1 Compruebe que los nodos pasivo y testigo se puedan alcanzar desde el nodo activo.

2 Compruebe que esté configurado correctamente el enrutamiento entre los nodos.

3 Compruebe la latencia de red.

Solucionar problemas de un clúster de vCenter HA degradado

Para que el estado de un clúster de vCenter HA sea correcto, cada uno de los nodos activo, pasivo y testigo deben estar totalmente operativos y se debe poder acceder a ellos mediante la red del clúster de vCenter HA. Si se produce un error en alguno de los nodos, se considera que el clúster se encuentra en estado degradado.

Problema

Si el clúster se encuentra en estado degradado, la conmutación por error no puede ocurrir. Si desea obtener información sobre los escenarios de error mientras el clúster se encuentra en estado degradado, consulte Resolver errores de conmutación por error.

Causa

El clúster puede estar en estado degradado por varios motivos.

Uno de los nodos tiene errores

- Si se produce un error en el nodo activo, se produce una conmutación por error del nodo activo al nodo pasivo de forma automática. Una vez que finaliza la conmutación por error, el nodo pasivo se convierte en el nodo activo.

  En este punto, el clúster se encuentra en un estado degradado porque el nodo activo original no se encuentra disponible.

  Una vez que el nodo con errores se repara o se conecta, se convierte en el nuevo nodo pasivo y el clúster vuelve a tener un estado correcto después de que los nodos activo y pasivo se sincronizan.

- Si se produce un error en el nodo pasivo, el nodo activo sigue funcionando, pero no se puede realizar la conmutación por error y el clúster está en estado degradado.

  Si el nodo pasivo se repara o se conecta, se vuelve a unir al clúster automáticamente, y el estado del clúster es correcto una vez que los nodos activo y pasivo se sincronizan.

- Si se produce un error en el nodo testigo, el nodo activo sigue funcionando y continúa la replicación entre el nodo activo y pasivo, pero no puede realizarse la conmutación por error.

  Si el nodo testigo se repara o se conecta, vuelve a unir el clúster automáticamente, y el estado del clúster es correcto.

La replicación de la base de datos presenta errores

Si se produce un error en la replicación entre los nodos activo y pasivo, se considera que el clúster está degradado. El nodo activo sigue sincronizándose con el nodo pasivo. Si el proceso se realiza correctamente, el clúster vuelve al estado correcto. Este estado puede originarse debido a problemas en el ancho de banda de la red u otras faltas de recursos.

Problemas de replicación de archivos de configuración

Si los archivos de configuración no se replican correctamente entre los nodos activo y pasivo, el clúster se encuentra en estado degradado. El nodo activo sigue intentando sincronizarse con el nodo pasivo. Este estado puede originarse debido a problemas en el ancho de banda de la red u otras faltas de recursos.

Solución

La manera en que se recupera depende de la causa del estado degradado del clúster. Si el clúster está en estado degradado, los eventos, las alarmas y las capturas de SNMP muestran errores.

Si se desactiva uno de los nodos, compruebe que no haya errores de hardware o que la red no esté aislada. Compruebe que el nodo con errores esté encendido.

En caso de que se produzcan errores de replicación, asegúrese de que la red de vCenter HA tenga suficiente ancho de banda y de que la latencia de red sea inferior a 10 ms.

Recuperarse de nodos de vCenter HA aislados

Si los nodos de un clúster de vCenter HA no pueden comunicarse entre sí, el nodo activo deja de procesar las solicitudes de los clientes.

Problema

El aislamiento de nodos es un problema de conectividad de red.

Solución

1. Intente resolver el problema de conectividad. Si puede restaurar la conectividad, los nodos aislados vuelven a unir el clúster automáticamente y el nodo activo comienza a procesar las solicitudes de los clientes.
2. Si no puede resolver el problema de conectividad, tiene que iniciar sesión en la consola del nodo activo directamente.
   a. Apague y elimine las máquinas virtuales del nodo pasivo y nodo testigo.
   b. Utilice SSH o la consola de la máquina virtual para iniciar sesión en el nodo activo.
   c. Para habilitar el shell Bash, introduzca **`shell`** en la solicitud `appliancesh`.
   d. Ejecute el siguiente comando para eliminar la configuración de vCenter HA.

      ```
      destroy-vcha -f
      ```

e Reinicie el nodo activo.

El nodo activo es ahora una instancia de vCenter Server Appliance independiente.

f Vuelva a realizar la configuración del clúster de vCenter HA.

Resolver errores de conmutación por error

Cuando un nodo pasivo no se convierte en nodo activo durante una conmutación por error, puede forzar el nodo pasivo para que se convierta en el nodo activo.

Problema

El nodo pasivo tiene errores cuando intenta asumir la función de nodo activo.

Causa

Es posible que las conmutaciones por error de vCenter HA no se realicen correctamente por los siguientes motivos.

- El nodo testigo no está disponible mientras el nodo pasivo intenta adoptar la función del nodo activo.
- Existe un problema de sincronización de estado del dispositivo entre los nodos.

Solución

Puede recuperarse de este problema de la siguiente manera.

1 Si el nodo activo se recupera del error, volverá a ser el nodo activo.

2 Si el nodo testigo se recupera del error, siga estos pasos.

   a Inicie sesión en el nodo pasivo a través de la consola de la máquina virtual.

   b Para habilitar el shell Bash, introduzca **`shell`** en la solicitud `appliancesh`.

   c Ejecute el siguiente comando.

   ```
   vcha-reset-primary
   ```

   d Reinicie el nodo pasivo.

3 Si tanto el nodo activo como el nodo testigo no pueden recuperarse, puede forzar el nodo pasivo para que se convierta en una instancia independiente de vCenter Server Appliance.

   a Elimine las máquinas virtuales del nodo activo y del nodo testigo.

   b Inicie sesión en el nodo pasivo a través de la consola de la máquina virtual.

   c Para habilitar el shell Bash, introduzca **`shell`** en la solicitud `appliancesh`.

   d Ejecute el siguiente comando.

   ```
   destroy-vcha
   ```

   e Reinicie el nodo pasivo.

Eventos y alarmas de VMware vCenter® HA

Si un clúster de vCenter HA está en estado degradado, los eventos y las alarmas muestran errores.

Problema

Tabla 4-4. Los siguientes eventos activan la alarma de estado de VCHA en vpxd:

Nombre del evento	Descripción del evento	Tipo de evento	Categoría
El estado actual del clúster de vCenter HA es correcto	El estado actual del clúster de vCenter HA es correcto	com.vmware.vcha.cluster.state.healthy	info
El estado actual del clúster de vCenter HA es degradado	El estado actual del clúster de vCenter HA es degradado	com.vmware.vcha.cluster.state.degraded	advertencia
El estado actual del clúster de vCenter HA es aislado	El estado actual del clúster de vCenter HA es aislado	com.vmware.vcha.cluster.state.isolated	error
El clúster de vCenter HA está destruido	El clúster de vCenter HA está destruido	com.vmware.vcha.cluster.state.destroyed	info

Tabla 4-5. Los siguientes eventos activan la alarma de estado de PSC en vpxd:

Nombre del evento	Descripción del evento	Tipo de evento	Categoría
El estado actual de PSC HA es correcto	El estado actual de PSC HA es correcto	com.vmware.vcha.psc.ha.health.healthy	info
El estado actual de PSC HA es degradado	El estado actual de PSC HA es degradado	com.vmware.vcha.psc.ha.health.degraded	info
PSC HA no se supervisa después de que se destruya el clúster de vCenter HA	No se está supervisando el estado de PSC HA	com.vmware.vcha.psc.ha.health.unknown	info

Tabla 4-6. Eventos relacionados con el estado del clúster

Nombre del evento	Descripción del evento	Tipo de evento	Categoría
El nodo {nodeName} se unió nuevamente al clúster	Un nodo se unió nuevamente al clúster	com.vmware.vcha.node.joined	info
El nodo {nodeName} abandonó el clúster	Un nodo abandonó el clúster	com.vmware.vcha.node.left	advertencia
La conmutación por error se realizó correctamente	La conmutación por error se realizó correctamente	com.vmware.vcha.failover.succeeded	info
No se puede continuar con la conmutación por error cuando el clúster está en modo deshabilitado	No se puede continuar con la conmutación por error cuando el clúster está en modo deshabilitado	com.vmware.vcha.failover.failed.disabled.mode	advertencia
No se puede continuar con la conmutación por error cuando el clúster no tiene los tres nodos conectados	No se puede continuar con la conmutación por error cuando el clúster no tiene los tres nodos conectados	com.vmware.vcha.failover.failed.node.lost	advertencia

Tabla 4-6. Eventos relacionados con el estado del clúster (continuación)

Nombre del evento	Descripción del evento	Tipo de evento	Categoría
No se puede continuar con la conmutación por error cuando vPostgres en el nodo pasivo no está listo para tomar el control	No se puede continuar con la conmutación por error cuando el nodo pasivo no está listo para tomar el control	com.vmware.vcha.failover.failed.passive.not.ready	advertencia
El modo del clúster de vCenter HA cambió a {clusterMode}	El modo del clúster de vCenter HA cambió	com.vmware.vcha.cluster.mode.changed	info

Tabla 4-7. Eventos relacionados con la replicación de la base de datos

Nombre del evento	Descripción del evento	Tipo de evento	Categoría
El modo de replicación de la base de datos cambió a {newState}	El estado de replicación de la base de datos pasó a ser síncrono, asíncrono o sin replicación	com.vmware.vcha.DB.replication.state.changed	info

Tabla 4-8. Eventos relacionados con la replicación de archivos

Nombre del evento	Descripción del evento	Tipo de evento	Categoría
El dispositivo {fileProviderType} está en estado {state}	El estado de replicación de archivos del dispositivo cambió	com.vmware.vcha.file.replication.state.changed	info

Aplicar revisiones en un entorno de vCenter High Availability

Es posible aplicar una revisión en una instancia de vCenter Server Appliance que se encuentra en un clúster de vCenter High Availability mediante la utilidad **`software-packages`** disponible en el shell de vCenter Server Appliance.

Para obtener más información, consulte *Aplicar revisiones en un entorno de vCenter High Availability* en *Actualizar vSphere*.

Usar el servicio de agrupación en clústeres de Microsoft para vCenter Server en alta disponibilidad de Windows

5

Cuando implementa vCenter Server, debe construir una arquitectura altamente disponible que pueda manejar cargas de trabajo de todos los tamaños.

La disponibilidad es clave para las soluciones que requieren una conectividad continua con vCenter Server. A fin de evitar períodos de inactividad prolongados, puede lograr una conectividad continua para vCenter Server mediante el clúster del servicio de clústeres de Microsoft (MSCS).

Este capítulo incluye los siguientes temas:

Beneficios y limitaciones del uso de MSCS

La actualización 3.x de vCenter Server 5.5 admite el servicio de clúster de Microsoft (MSCS) como opción para proporcionar disponibilidad de vCenter Server.

Existen varias instancias de vCenter Server en un clúster de MSCS, pero solo una instancia está activa a la vez. Utilice esta solución para realizar tareas de mantenimiento, como la aplicación de revisiones y actualizaciones del sistema operativo, sin incluir la aplicación de revisiones y actualizaciones de vCenter Server. El mantenimiento se realiza en un nodo del clúster sin desconectarse de la base de datos de vCenter Server.

Otro posible beneficio de este enfoque es que MSCS usa un tipo de arquitectura de clúster "que no comparte nada". El clúster no implica accesos simultáneos al disco desde varios nodos. En otras palabras, el clúster no requiere un administrador de bloqueo distribuido. Comúnmente, los clústeres de MSCS incluyen solo dos nodos y usan una conexión SCSI compartida entre los nodos. Solo un servidor necesita los discos en algún momento determinado. No se produce acceso simultáneo a los datos. Este uso compartido minimiza el impacto en caso de error del nodo.

A diferencia de la opción del clúster de vSphere HA, la opción de MSCS funciona únicamente para las máquinas virtuales de Windows. La opción de MSCS no admite vCenter Server Appliance.

Nota Esta configuración solo se admite cuando vCenter Server se está ejecutando como una máquina virtual, no en un host físico.

Actualizar vCenter Server en un entorno MSCS

Si está ejecutando vCenter Server 6.0, debe actualizar a vCenter Server 6.5 para establecer un entorno MSCS de alta disponibilidad.

vCenter Server 6.0 x tiene 18 servicios, si se asume que el servidor PSC se está ejecutando en un host distinto. vCenter Server 6.5 tiene tres servicios cuyos nombres se cambiaron. Una configuración de clúster de MSCS creada para configurar alta disponibilidad para vCenter Server 6.0 deja de tener validez después de una actualización a vCenter Server 6.5.

El proceso para configurar alta disponibilidad para vCenter Server en un entorno MSCS es el siguiente.

1 Elimine la configuración de MSCS para vCenter Server.

2 Actualice vCenter Server de la versión 6.0 a la versión 6.5.

3 Configure MSCS para que vCenter Server tenga alta disponibilidad.

Requisitos previos

- Compruebe que no se elimina la máquina virtual del nodo principal.
- Compruebe que el nodo principal sea el nodo activo actual.
- Compruebe que todos los servicios de vCenter Server 6.0 se estén ejecutando en el nodo principal.
- Compruebe que la actualización del nodo Platform Services Controller se haya completado y que se esté ejecutando vCenter Server 6.5.
- Recopile la copia de seguridad de la base de datos del inventario.

Procedimiento

1 Apague el nodo secundario y espere a que todos los servicios de vCenter Server se inicien en el nodo principal.

2 Elimine el nombre de la función.

3 Destruya el clúster de MSCS. Vuelva a conectar los discos RDM antes de cambiar el tipo de inicio.

4 Abra la vista Administración de servicio y cambie el tipo de inicio de los servicios de vCenter Server de manual a automático.

5. Antes de actualizar a vCenter Server 6.5, cambie el IP y el nombre del host por el IP y el nombre del host utilizados para la función.

   Debe reiniciar el host y asegurarse de que se pueda acceder a vCenter Server.

6. Monte la imagen ISO de vCenter Server 6.5 e inicie la instalación.
7. Una vez que finalice la instalación, abra la vista Administración de servicio y compruebe que los servicios nuevos estén instalados y que se estén ejecutando.
8. Vuelva a configurar el clúster de MSCS y establezca el tipo de inicio de todos los servicios de vCenter Server en manual.
9. Desconecte el nodo principal y separe los discos RDM, pero no los elimine del almacén de datos.
10. Una vez que se configure, seleccione **Máquina virtual > Clonar > Clonar a plantilla**, clone el nodo secundario, y cambie su IP y nombre de host.
11. Mantenga el nodo secundario apagado y agregue los dos discos RDM al nodo principal. A continuación, encienda el nodo principal, y cambie su IP y nombre de host.
12. Agregue los dos discos RDM al nodo secundario. A continuación, encienda el nodo secundario.
13. Abra el Administrador de clústeres de conmutación por error y configure el clúster de MSCS.

    Debe utilizar el IP y el nombre de host de la función del clúster.

Pasos siguientes

Al configurar el clúster de MSCS, debe agregar servicios de vCenter Server, como el servicio VMware AFD y el servicio VMware vCenter Configuration a la función como recursos.

Configurar MSCS para alta disponibilidad

Utilice los siguientes pasos para configurar Servicio de clúster de Microsoft (MSCS) como una solución de disponibilidad para vCenter Server.

Requisitos previos

- Cree una máquina virtual con uno de los siguientes sistemas operativos invitados:
- - Windows 2008 R2 Datacenter
  - Windows 2012 R2 Datacenter
- Agregue dos discos con asignaciones de dispositivos sin procesar (Raw Device Mapping, RDM) a esta máquina virtual. Estos discos deben estar montados cuando se agregan y los discos RDM también deben ser independientes y persistentes.

- Cree un controlador SCSI distinto con la opción de uso compartido de bus establecida en físico.

  Nota Debido a que esta configuración usa un controlador SCSI con la opción Uso compartido de bus establecida en Físico, la copia de seguridad y la restauración no son compatibles. Debe usar un agente basado en host para la copia de seguridad o la restauración.

- Establezca el nodo de dispositivo virtual en el controlador SCSI 1 recientemente creado.
- Abra la unidad MSCS y cree dos carpetas: una para datos de VC y otra para la instalación de VC.
- Instale una instancia de Platform Services Controller antes de instalar vCenter Server y proporcione su FQDN durante la instalación.

Figura 5-1. Clúster MSCS para alta disponibilidad de vCenter Server

Nodo de infraestructura de vCenter Server (VM1) N1
Nodo de infraestructura de vCenter Server (VM2) N2
Nodo de administración de vCenter Server (VM1) M1
Nodo de administración de vCenter Server (VM2) M1
Clúster de MSCS
Base de datos de SQL Server (VM1) Nodo 1
Base de datos de SQL Server (VM2) Nodo 2
Clúster de MSCS

Nota MSCS como una solución de disponibilidad para vCenter Server se proporciona únicamente para los nodos de administración de vCenter Server (nodo M). Para los nodos de infraestructura, los clientes deben implementar varios nodos N para alcanzar una alta disponibilidad. No es posible tener nodos M y N en la misma máquina virtual para la protección MSCS.

Procedimiento

1. Encienda la máquina virtual.
2. Formatee los 2 discos RDM, asígneles letras de unidad y conviértalos a MBR.
3. Utilice **Windows > Administrador del servidor > Características** e instale .net.
4. Instale vCenter Server en uno de los discos RDM y establezca la opción de inicio en manual.
5. Apague la máquina virtual.

6 Separe los discos RDM.

   Separar los discos RDM no es una eliminación permanente. No seleccione **Eliminar del disco** ni elimine los archivos vmdk.

7 Clone la máquina virtual. No seleccione la opción **Personalizar el sistema operativo**.

   No utilice el archivo sysprep personalizado ni el predeterminado, de manera que el clon tenga el mismo SID.

   Nota La generalización por sysprep no está disponible cuando se crea una máquina virtual clonada como el nodo secundario de un clúster. Si utiliza la generalización por sysprep, puede producirse un error en la conmutación por error de los servicios al nodo secundario. SID duplicados no causan problemas cuando los hosts forman parte de un dominio y solo se usan cuentas de usuario de dominio. No se recomienda la instalación de software de terceros que no sea vCenter Server en el nodo del clúster.

   ---

8 Asocie los RDM compartidos a ambas máquinas virtuales y enciéndalas.

9 Cambie el nombre del host y la dirección IP en la primera máquina virtual (VM1).

   Tenga en cuenta la dirección IP y el nombre del host original que se utilizaron en el momento de la instalación de vCenter Server en la primera máquina virtual (VM1). Esta información se utiliza para asignar una dirección IP de rol de clúster.

10 Instale los clústeres de conmutación por error en ambos nodos.

11 Para crear un clúster MSCS en la primera máquina virtual (VM1), incluya ambos nodos en el clúster. También seleccione la opción de validación para el clúster nuevo.

12 Para comenzar a configurar funciones, seleccione **Servicio genérico** y haga clic en **Siguiente**.

13 Seleccione **VMware Service Lifecycle Manager** en los servicios que aparecen y haga clic en **Siguiente**.

14 Introduzca el nombre de host y la IP usados para la VM1. A continuación, asigne el RDM a la función.

15 En el asistente Configuración de registro de replicación, agregue la clave de registro **`SYSTEM\CurrentControlSet\Services\VMwareDirectoryService`** y haga clic en **Siguiente**.

16 Con la opción para agregar un recurso, agregue los servicios VMware AFD y VMware vCenter Configuration a la función.

17 Detenga y reinicie la función.

Resultados

Ha creado un clúster MSCS que puede admitir la disponibilidad de vCenter Server.

Pasos siguientes

Después de haber creado el clúster MSCS, compruebe que se esté produciendo la conmutación por error. Para ello, apague la máquina virtual que hospeda a vCenter Server (VM1). Espere algunos minutos y compruebe que los servicios se estén ejecutando en la otra máquina virtual (VM2).